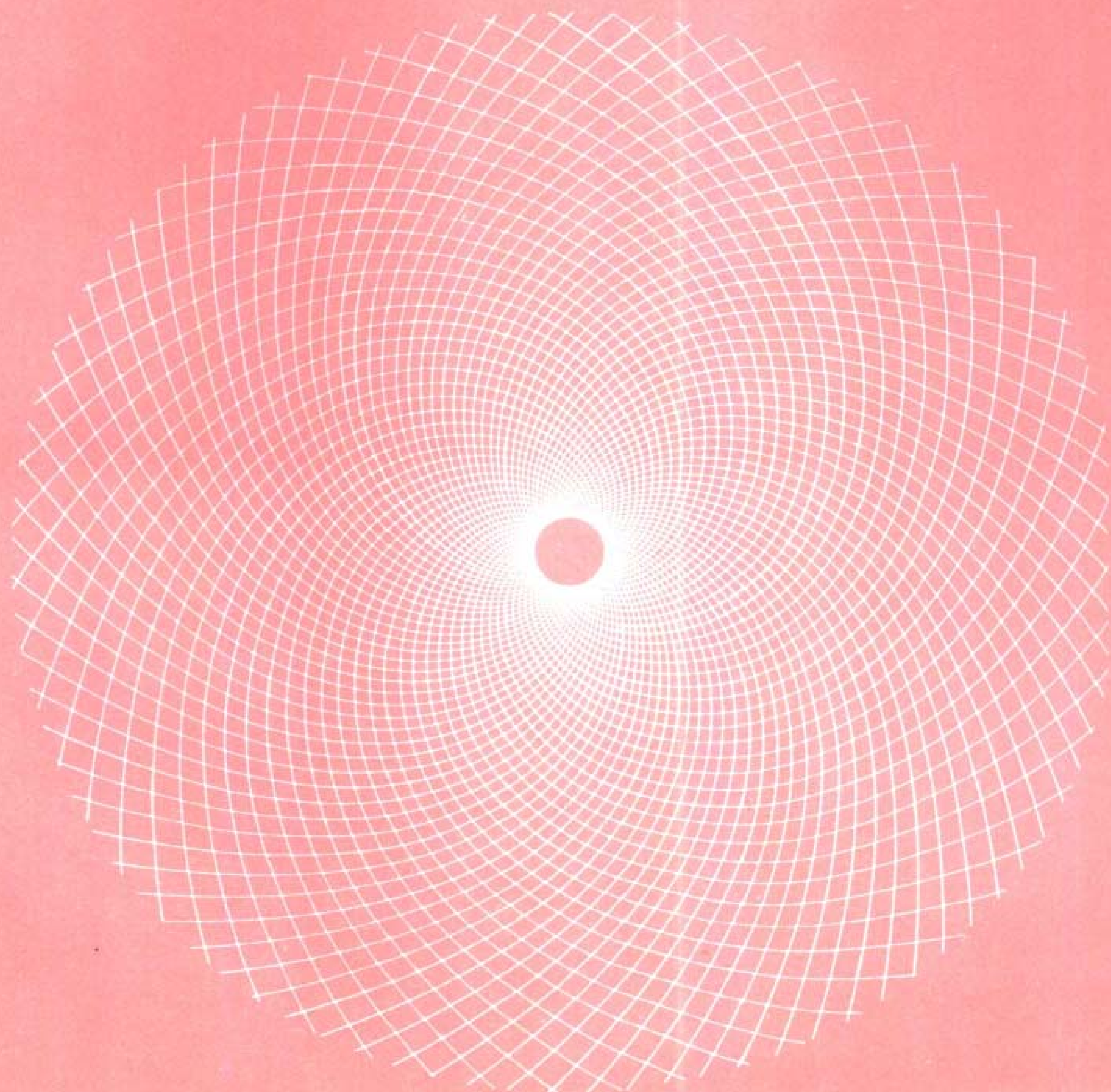
数论妙趣
——数学女王的盛情款待

[美]阿尔伯特·H·贝勒著　谈祥柏译　●　上海教育出版社



图书在版编目（CIP）数据

数论妙趣：数学女王的盛情款待 / （美）贝勒著：谈祥柏译. —上海：上海教育出版社，1998.1（2000.3重印）
（通俗数学名著译丛 / 史树中，李文林主编）
ISBN 7-5320-5473-X

Ⅰ.数... Ⅱ.①贝...②谈... Ⅲ.数论-通俗读物
Ⅳ.O156-49

中国版本图书馆CIP数据核字（2000）第15862号

Albert H. Beiler

Recreations In The Theory of Numbers

The Queen of Mathematics Entertains

Dover Publications, INC.

根据多佛出版社1964年第1版译出，
本书中文版权由上海市版权代理公司帮助取得

通俗数学名著译丛

数论妙趣

——数学女王的盛情款待

[美]阿尔伯特·H·贝勒 著

谈 柏 祥 译

上海世纪出版集团
上海教育出版社 出版发行

（上海永福路123号 邮政编码：200031）

各地新华书店经销 上海市印刷三厂印刷

开本 850×1156 1/32 印张 14 插页 5 字数 332,000

1998年1月第1版 2000年3月第4次印刷

印数 9,221—14,220本

ISBN 7-5320-5473-X/G·5715 定价：18.80元

译丛序言

数学，这门古老而又常新的科学，正阔步迈向21世纪.

回顾即将过去的世纪，数学科学的巨大发展，比以往任何时代都更牢固地确立了它作为整个科学技术的基础的地位. 数学正突破传统的应用范围向几乎所有的人类知识领域渗透，并越来越直接地为人类物质生产与日常生活作出贡献. 同时，数学作为一种文化，已成为人类文明进步的标志. 因此，对于当今社会每一个有文化的人士而言，不论他从事何种职业，都需要学习数学，了解数学和运用数学. 现代社会对数学的这种需要，在未来的世纪中无疑将更加与日俱增.

另一方面，20世纪数学思想的深刻变革，已将这门科学的核心部分引向高度抽象化的道路. 面对各种深奥的数学理论和复杂的数学方法，门外汉往往只好望而却步. 这样，提高数学的可接受度，就成为一种当务之急. 尤其是当世纪转折之际，世界各国都十分重视并大力加强数学的普及工作，国际数学联盟（IMU）还专门将2000年定为**“世界数学年”**，其主要宗旨就是“使数学及其对世界的意义被社会所了解，特别是被普通公众所了解”.

一般说来，一个国家数学普及的程度与该国数学发展的水平相应并且是数学水平提高的基础. 随着中国现代数学研究与教育的长足进步，数学普及工作在我国也受到重视. 早在60年代，华罗庚、吴文俊等一批数学家亲自动手撰写的数学通俗读

物，激发了一代青少年学习数学的兴趣，影响绵延至今.改革开放以来，我国数学界对传播现代数学又作出了新的努力.但总体来说，我国的数学普及工作与发达国家相比尚有差距.我国数学要在下世纪初率先赶超世界先进水平，数学普及与传播方面的赶超乃是一个重要的环节和迫切的任务.为此，借鉴外国的先进经验是必不可少的.

《通俗数学名著译丛》的编辑出版，正是要通过翻译、引进国外优秀数学科普读物，推动国内的数学普及与传播工作，为我国数学赶超世界先进水平的跨世纪工程贡献力量.丛书的选题计划，是出版社与编委会在对国外数学科普读物广泛调研的基础上讨论确定的.所选著述，基本上都是在国外已广为流传、受到公众好评的佳作.它们在内容上包括了不同的种类，有的深入浅出介绍当代数学的重大成就与应用；有的循循善诱启迪数学思维与发现技巧；有的富于哲理阐释数学与自然或其他科学的联系；……等等，试图为人们提供全新的观察视角，以窥探现代数学的发展概貌，领略数学文化的丰富多采.

丛书的读者对象，力求定位于尽可能广泛的范围.为此丛书中适当纳入了不同层次的作品，以使包括大、中学生；大、中学教师；研究生；一般科技工作者等在内的广大读者都能开卷受益.即使是对于专业数学工作者，本丛书的部分作品也是值得一读的.现代数学是一株分支众多的大树，一个数学家对于他所研究的专业以外的领域，也往往深有隔行如隔山之感，也需要涉猎其他分支的进展，了解数学不同分支的联系.

需要指出的是，由于种种原因，近年来国内科技译著尤其是科普译著的出版并不景气，有关选题逐年减少，品种数量不断下降.在这样的情况下，上海教育出版社以迎接2000世界数学年为契机，按照国际版权公约，不惜耗资购买版权，组织翻译出版这套《通俗数学名著译丛》，这无疑是值得称道和支持的举措.参加本丛书翻译的专家学者们，自愿抽出宝贵的时间来进行这类

通常不被算作成果但却能帮助公众了解和欣赏数学成果的有益工作，同样也是值得肯定与提倡的.

像这样集中地翻译、引进数学科普读物，在国内还不多见. 我们热切希望广大数学工作者和科普工作者来关心、扶植这项工作，使《通俗数学名著译丛》出版成功.

让我们举手迎接 2000 世界数学年，让公众了解、喜爱数学，让数学走进千家万户！

《通俗数学名著译丛》编委会
1997 年 8 月

献给

克利丝

数学是科学的女王，而算术则是数学的女王.

——卡尔·弗里特列希·高斯

序

当作者还是一个学生时，一位热心的数学教授向全班介绍了W·W·R·鲍尔(W. W. R. Ball)所写的一本书《数学娱乐与随笔》. 学生们顺从地记下了书名，绝大多数人无疑转眼就忘得干干净净. 多年之后，当作者向自己的几个班级提到这本书时，学生们却出乎意外地对书名表示喜爱，并随之引发了一系列的质问，"娱乐"与"数学"是互相抵触的字眼，怎能合在一起呢？这是一群工科大学生的反应，他们对数学的熟练程度在平均水平之上，那么，对一大群并非出于自觉自愿，而是被迫学习数学的人，他们的态度又将如何呢？

尽管事先并不看好，结果发现，仅仅提到几个趣题，就立即使全班学生从出了名的厌学与昏睡中惊醒过来，同数论有关的一个问题竟导致非常热烈的反响以致学生们竟然不愿再回复他们的正常课业. 这些问题的刺激力在全班持续了很长时间，为此，代数、三角、解析几何、微积分的规定作业也增添了兴趣. 它像是一种催化剂，本身虽然不参加化学反应，却把其他物质激活了.

对一些缺乏数学细胞的朋友(尽管如此，他们还是要曝晒在高中代数之下活活受罪)进行了相当谨慎的实验，引起的反响也同样令人满意，这就使作者产生了编写本书的想法.

一些数学家，例如W·W·R·鲍尔与E·卢卡(Lucas)等人曾写过质量一流的、一般题材的趣味数学读物；其他一些学

者,例如托比亚斯·但捷格(Tobias Dantzig),E·T·贝尔(Bell),爱德华·卡斯纳(Edward Kasner)则写过一些异常优秀的、介绍数学概念以及数学家传记之类的作品.但是,在英文书里,却缺少一本专讲趣味数论的书,本书试图弥补这个缺陷,为大家提供一些趣味盎然的奇珍异宝.还可以在任何一个收藏着很多数学书刊的大图书馆里,找到隐藏在枯燥乏味的技术论文底层的、为数更多的宝贝.

数论之所以具有难以抗拒的魅力,其中很重要的一个原因是它的问题浅显易懂,但特别迷人.另外,它又并不需要过多的预备知识.只要掌握一般高中程度的数学基础知识,初学者即可登堂入室,理解它的许多重要内容.正像读过几部侦探小说的人会情不自禁地觉得自己已有了足够的本领,可以帮助警方侦破谋杀案一样,数论领域里的初学者身上很快就会长出伊卡鲁斯之翼①,在原根与二次剩余中自由翱翔.

数学家卡尔·弗里德列希·高斯(Karl Friedrich Gauss)曾经说过:"高等算术中一些最美丽的定理具有这样的特性:它们极易从经验事实中归纳出来,但其证明却隐藏得极深,只有高人一等的研究者才能把它们挖掘出来.正是出于此种原因,赋予高等算术以神奇魅力,使之成为第一流数学家们最喜爱的科学.至于它远远凌驾于数学其他各分支之上的无限丰富性,那就更不必提了."

作者经常遇到的两难处境是:究竟要不要讲一讲本书各个章节所涉及的理论知识,还是干脆将它删除?如果理论讲得太多,这本书就再无趣味可言.反之,理论说明往往同结果一样有滋味——有时甚至更好.基于这样一种考虑,本书还是收入了相当数量的理论性内容.读者可根据自己的爱好,或读或删.

---

① 伊卡鲁斯是希腊神话中的人物,他能用蜡造的翼高翔空中.后来,他在飞到太阳附近时,蜡制的翼受热融化,堕海而死.——译者注.

一般地说，书中后面几章的内容要比前几章深奥一些，所以建议读者还是按照各章的先后顺序进行阅读. 为了增加阅读兴趣，问题是星罗棋布地分散在各章之中的. 如在问题之后未见答案，则它在第26章中总可以找到. 第25章专门列出了一百个问题，它们的解答与解法提示也包含在最后一章之中.

梅森数，清一色的111…1，以及费马数(这些题材分别在第3，第11与第17章中阐述)的因子在近几年中又新发现了不少. 由于时间紧迫，本书来不及将它们收入进去. 读者可参看《计算数学》杂志，第17卷(1963年)447，458页.

阿尔伯特·H·贝勒

1963年写于纽约

内 容 简 介

本书不仅包括平面自治系统与稳定性理论初步，而且还较系统地阐述了不少学科所需要的常微分方程分支理论. 全书共十三章，有：基本定理、二维系统的平衡点、二维系统的极限环、动力系统、振动方程与生态方程、n 维系统的平衡点、多重奇点的分支、Hopf 分支、从闭轨分支出极限环、同宿分支及异宿分支、高维问题、综合应用，以及柱面与环面上的动力系统及其应用. 书末附有 90 余道习题.

本书可作为高等学校数学系高年级及研究生教材或教学参考书，也可供物理、化学、生物等有关方面科学技术工作者参考.

目　录

插　图

图版

附 表

数 论 妙 趣

——数学女王的盛情款待

以此短文作为前言的这本数学课本……与世上任何一本算术书都不一样.书中没有很大的数目,很大的数目……将对人们的想象能力施加不利影响,有害于社交活动,而又脱离实际.它像是中了邪的恶魔,不断发出有毒气体,腐蚀与败坏了粉红色的大脑的正常运转.

这本书里头有着许许多多7与3……7与3很吸引人,7使我们称心如意……天上有七姐妹星团[①],还有七座山,七位苏德兰姐妹……[嫁给七兄弟的七位新娘].

——唐·马奎斯

"一本算术德育书的序言"

① 即昴宿星团.——译者注.

第1章 宫廷亮相

趣题爱好者将会发现数论是大量赏心悦目而且无穷无尽的趣题之源.这一领域被人捧为"数学之女王"(而数学本身则是"科学的女王"),其中熠熠发光地闪耀着世上第一流数学家们奉献出来的智慧珍宝.探索一些具有特殊性质的奇异数字有着一种不可抗拒的魔力,一经投入其中,人们即会对其魔法顶礼膜拜并终于理解何以有如此多的人愿意在此课题上投入大量时间.在追求数论中的一些扰人课题时,再也没有比"生命短暂,艺术长存"这句拉丁格言更加确切了.

对解决以下问题,你是不是打算有所作为?

1. 求出数 16000001 的一切除数.† ①

2. 直角三角边的某一边之长为 48.试写出十对正整数,其中每一对是该三角形中另外两边之长.†

3. 小于 5929 且与之互质的正整数一共有多少? †

4. 试求出一个最小的,完全由数码 3 与 7 构成的正整数,此数以及其数字和均能被 3 与 7 整除.†

5. 求出能形成算术级数的三个平方数.四个行不行? †

6. 求出一个恰好拥有 100 个除数的最小数.†

7. 证明当 n 为素数时,$1\cdot2\cdot3\cdot4\cdot\cdots\cdot(n-1)+1$ 必能

① 有†记号的问题,其解法可参阅第 26 章.——原注.

被 n 整除,但当 n 为合数时,决不能整除.†

8. 证明形如 $4x+1$ 的任一素数必能唯一地表示为两个平方数之和.†

[1] 9. 找出一些数,其中的每一个都等于其不同除数之和(所谓除数,其中应包括 1,但不包括此数本身).†

10. 找出 x 值的一般公式,使 2^x-1 得出素数.†

11. 证明任一偶数都可表为两个素数之和.†

12. 证明 $n>2$ 时,$x^n+y^n=z^n$ 不可能有整数解.

中等水平的高中学生都能理解这些问题的要求,但其中某些问题的实际求解却抵挡住了许多世纪的智力攻势,至今仍然屹立不动.这就是问题 10,问题 11 与问题 12.光是问题 10 的历史沿革,就能为它专门写一本书,要想把花在这上面的工作网罗无遗,那就还得写上好多卷大书.与问题 12 有关的资料为数极其庞大.问题 8 需要机智的解析.问题 2 与 5 涉及数论的一个分支——丢番图分析,这一学科由丢番图(Diophantus)而得名,其人为早年基督教传播时期的一位数学家.仅仅是丢图番分析的历史,在 L·E·狄克逊(Dickson)的煌煌巨著中,就占了 700 多页的篇幅.

数论与数学的其他分支很不一样,它几乎纯粹是一门理论性学科.某些杰出的科学家或工程师偶然会把它的一些基础定理投入实际应用:例如电话线的捻接,立方晶体的 X 射线波谱分析以及某些无线电技术.但从总体情况看来,它是远离世俗,超然物外的.据说一位伟大的追随者库默(E. E. Kummer)在某个场合曾经说过,在他所有的发现中,他特别欣赏的是他的"理想数",主要是由于它从未被任何实际应用所玷污.

数学的其他分支里没有如此热情的执着追求者.大卫·希尔伯特(David Hilbert)在其对莱德(L. W. Reid)所著的《代数数论基础》一书的序言中写道:"在数论中,我们非常看重其基础

的简洁，概念的完整确切，论断的纯粹；我们要为它大声歌颂：它是其他科学的典范；一切数学知识的最深刻、永不涸竭的源泉；它总是毫不吝惜地鼓动其他数学分支的深入研究……另外，数论不受流行时尚的影响，在它那里几乎看不到别的知识部门频频发生的情况，一种概念或方法忽然红得发紫，忽而又被打入冷宫，受到不应有的忽视. 在数论里，历史上最古老的问题往往是今日最时髦的，犹似往昔年代一件真正的艺术佳构.” [2]

L·E·狄克逊在其划时代的巨著《数论史》中说道：“数论特别有资格为之列出专章讲述其历史沿革，这是因为从毕达哥拉斯时期开始，它已连续好多世纪吸引了世人的巨大兴趣；其一头是几乎每一位著名数学家，另一头则是广大业余爱好者，而在数学的其他分支，这种现象是看不到的.”

一位著名数学家兼数论专家哈代(G. H. Hardy)说过：“初等数论应当是一种极好的早期数学教育素材. 它需要的预备知识很少，材料很实在，可以触摸得到，又为人们所熟悉；它所用的推理过程非常简单，有普遍意义，而且为数不多；在数学科学中它非常独特，因为它能激发人们的天然好奇心. 花上一个月时光，进行富有智慧的数论启蒙教育，它将会带来双倍效益，双倍作用，比起同等数量的给工程技术人员上的微积分来说，更将是十倍地有趣.”①

人们进入这个数的世界，胆怯地在整数、除数、素数里面徘徊漫步，这些名词，半生半熟，模糊地回忆起从前在小学校里读过的算术课. 我们很快就遇上了完全数与亲和数，接着是数的除数以及它们的和. 前面的迷人小径向人们招着手，把他们吸引到新的、以前未曾到过的同余式世界，然后便是费马(Fermat)定理与威尔逊(Wilson)定理的荆棘林莽. 原根，平方剩余，丢番图解析，主指数，以及二次互反律不断向我们呈现. 它们十分吸引

① 引自《美国数学会公报》，35卷(1929年)，818页. ——原注.

人,以致使我们不愿意离去.再向前去,山路越来越崎岖,进展非常迟缓,十分困难,它们是:二次型、分划,理想数与示性数,佩尔(Pell)方程,连分数,自同构,素数论以及解析数论.只有那些心智特别精灵之人才愿意继续往上攀登,到达更清洁,更纯粹,更光明的境界.在我们这本书里,将不去探索这些高峻而巍峨的绝顶,而只想在纯属娱乐性的国度里逍遥自在一番.

你想不想去作这次旅游呢?并不需要很多装备,主要是自己的一颗真正愿心.它将是有趣的,因为世上的一些祸害在我们门[3]前鼓噪不休,它也许是希腊神话里的一帖忘忧药——吃下去之后就能到达詹姆士·希尔顿(James Hilton)在《失去的地平线》这部小说里头所描写的、远在天涯海角的香格里拉.①

* * *

如果我们打算作一次愉快的远足,为了旅途愉快,需要有点装备.我们也许要购买一些新的用品,对已有的东西要好好翻修一下.到数世界去旅行,也需要一些装备,但数量并不很多.初等代数是非常有用的;几何知识不要求很全面,只要了解正方形的意义,三角形的各种不同类型,以及圆的若干知识就够了.对我们已经生了锈的算术装备进行全面检修看来十分必要.先去查查辞典,以了解整数,数码,素数,合数,因子,除数……的意义,作好这样的准备工作是可取的.

所谓一个**数码**,是指 0,1,2,3,4,5,6,7,8,9 中的一个,这一说法来自手指计数.诸如 15 之类的数称为**整数**,以区别于 7/3 这类分数.整数 15 记为数码 1 与数码 5.数 15 是一个**合数**,因为它是由两个因子(或除数)3 与 5 组成的.像 13,97 或者 67280421310721 这样的数称为**素数**,它们除了 1 与本身之外没有其他因子.迄今尚未发现判定一个数是否素数的一般方法.像

① 香格里拉即世外桃源或乌托邦;第二次世界大战时的美国陆军航空队的秘密基地.——译者注.

上面所列举的这一 14 位数字，除非它属于某种特殊类型，一般需要花费穷年累月的不懈努力，才能最终判明它是否素数.

我们的孩提时代，从整数进入分数，需要逾越一个不小的心理障碍. 也许我们中间的某些人能回忆得起家长的教诲："把一只饼分成五块，取走其中的三块，这就代表分数3/5."后来我们又跳过了更加众多的障碍物：不光是割断了两个整数之间的间隔以得到分数，而且在分数之间也有缺口，得出之数非此非彼. 我们把它们称为*无理数*. 单位正方形中对角线的长度经常被作为这种数的例证. 久而久之，在我们的心底里终于逐步形成了连续数流的概念.

但在数论里我们又回复到原始的概念. 我们扬弃"连续性"而考虑"离散量"，这并不意味着这种离散的量可以达到自我完善的境地，而毋宁是主张两个相邻的自然数是相互隔开的，不相连接的. 例如，在 14 与 15 之间不存在其他整数，而在 15 与 20 [4] 之间只存在四个其他整数.

由于数论只研究整数之类的离散量，所以它需要一种特殊观点与工具来处理它的问题. 求解的道路经常与代数问题平行，甚至吻合——但是这种貌似性相当危险，因为人们若不密切注视其区别，势将误入歧途. 以后，我们在讲解同余式与方程的异同，以及不同数域中的整数时，大家是会看到的.

现在让我们看一个问题：求不定方程 $5x+3y=17$ 中 x 与 y 的正数解. 从代数观点来说，存在着无限多组 x 与 y 值以满足该方程，这些解中，既有分数的，也有整数的，它们都对应于作为其图象的直线上的无限多个点. 但是，在数论领域中，我们只考虑 $x=1, y=4$ 作为这一方程的整数解.

让我们引用乌思宾斯基(Uspensky)与希斯莱特(Heaslet)的名著《基础数论》中的一段话，以结束数学女王宫廷中的引见[①]：

① 可参看 J. V. Uspensky 与 M. A. Heaslet 的《基础数论》，纽约，McGraw-Hill 图书公司 1939 年版. ——原注.

"究竟是什么力量驱使人们糜费大量时间与精力去从事算术研究?……答案是,只有在这个分支中钻研得很深的人才能揭露这门科学的整体完美性……

在人们得以鉴赏埋藏于其中的算术宝藏之前,自然需要掌握一些本身并不很有趣的事物与知识.不过,这是必不可少的:在学会走路之前,必须先学会爬行.

因而,在直立行走以及转过脸来投向光明之前,我们当然不可避免地需要先爬行一番.

参考文献[①]

Ball, W. W. R. *Mathematical Recreations and Essays.* New York: Macmillan Co., 1939.

Dickson, L. E. *History of the Theory of Numbers.* 3 vols. [5] New York: Chelsea Publishing Co., 1950.

Hardy, G. H. "An Introduction to the Theory of Numbers," *Bulletin of the American Mathematical Society*, **35** (1929), 778.

Lawther, H. P., Jr. "An Application of Number Theory to the Splicing of Telephone Cables," *American Mathematical Monthly*, **42** (1935), 81.

Reid, L. W. *Elements of the Theory of Algebraic Numbers.* Baltimore: Johns Hopkins Press, 1946.

Uspensky, J. V., and Heaslet, M. A. *Elementary Number*

① 在本章及以后各章的末尾,作者将尽量提供有关参考文献的重印件或最近资料,而不一定是原始论文.其目的是为了方便读者,以使他能够随时查到最容易到手的资料.——原注.

Theory. New York: McGraw-Hill Book Company, 1939.

Van Der Pol, B. "Radio Technology and Theory of Numbers," *Journal of the Franklin Institute*, **255**(1953), 475. [6]

第2章　除数好散心

当然你们很熟悉除数的一切. 如果要你列举某一数的除数，譬如说 24，那你就会写出 1，2，3，4，6，8，12，24，一共有 8 个除数. 你能不能不必一一列举而马上回答 24 有 8 个除数而 60 有 12 个呢? 要做到这一点必须首先把已知数分解成"基本构件"或者说其质因子乘幂的连乘积，而分解法是唯一的. 例如 $24=2^3\cdot 3$，$60=2^2\cdot 3\cdot 5$. 接着，再把每个质因子的乘幂加上 1，并连乘起来. 例如，在数 24 的质因子乘积中，2 与 3 的乘幂分别为 3 与 1，从而就有 $(3+1)(1+1)=8$ 个除数. 而对 60 来说，则有 $(2+1)(1+1)(1+1)=12$ 个除数.

如用一般的紧凑记法，数 $N=p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$，这里的 p_i 是相异素数，则 N 的除数个数应为

$$(a_1+1)(a_2+1)\cdots(a_n+1).$$

不要害怕下标. p 是史密斯家族的，a 是琼斯家族的. 比尔·史密斯，芬尼·史密斯，约翰·史密斯相当于 p_1，p_2，p_3；而玛丽·琼斯、汤姆·琼斯，珍妮·琼斯相当于 a_1，a_2，a_3. 我们也可把不同的素数称为 p，q，r，但较难表达它们都是素数家族中的一员. 下标可以区分家族成员，而同样的下标则表明该两家族的相应成员具有婚姻关系.

接下来便是相反的问题. 试求出一个数，它正好具有 14 个约数. 由于 $14=2\cdot 7$，把每个因子都减去 1，于是得到 1 与 6，可

把它们视为乘幂，配属于我们想取的任意素数. 一般说，要想得到最小的答案，就要取最小的素数. 就本例而言，可利用 2 与 3. 于是可得到 $2^6 \cdot 3^1 = 192$；与此同时，任一形为 p^6q（p，q 为素数）的数都正好具有 14 个除数. 我们当然也可以把 14 分解为 $1 \cdot 14$，结果得出解 p^{13}，例如 $2^{13} = 8192$.

[7] 要求出一个最小的正整数，使之具有给定个数的除数，这并非都很简单. 例如，若 12 是给定的除数个数，而我们写出 $12 = 2 \cdot 6$，这时，相应的指数为 1 与 5，而解是 $2^5 \cdot 3 = 96$，但 12 也可写成 $3 \cdot 4$，此时指数为 2 与 3，而解是 $2^3 \cdot 3^2 = 72$. 这些答案都比 60 来得大，而上文已说过，60 是正好具有 12 个除数的. 这个特殊的解是怎么找到的呢？原来，12 也可写成 $2 \cdot 2 \cdot 3$，这就给出对应指数为 1，1，2 而合乎题意的解，它便是 $2^2 \cdot 3 \cdot 5 = 60$.

读者们也许愿意去解第一章的问题 6：求一个正好具有 100 个除数的最小数；求出之后，再比较一下恰有 96 个除数的最小数. †①

数的除数之和可以引发许多有趣问题. 对此类问题而言，1 与此数本身也算作除数；如果该数本身不包括在内，那就称之为“真除数”(aliquot divisor)，其意思是指，小于此数的一切除数，当然其中也包括 1.

有关的一类趣题是：要找出一个正整数，使其除数之和恰为一个完全平方数. 满足此项要求的最小数是 3，因为 $1+3=4$，下一个数是 22，这是因为

$$1 + 2 + 11 + 22 = 36 = 6^2.$$

这问题很奥妙，因为即便掌握了某数的除数和公式，解决起来还是要靠经验方法. 具有此种性质的数有如下表：

① 带有† 记号问题的解法请参阅第 26 章. ——原注.

正整数	除数	除数和＝平方数
66	1;2;3;6;11;22;33;66	$144=12^2$
70	1;2;5;7;10;14;35;70	$144=12^2$
81	1;3;9;27;81	$121=11^2$
1501	1;19;79;1501	$1600=40^2$
4479865	1;5;13;41;65;205;533;1681;2665;8405;21853;68921;109265;344605;895973;4479865	$5934096=2436^2$

[8]

表 1　除数和恰为平方数的某些正整数

1657 年，大数学家费马提出如下问题：试找出一个立方数，在它加上其真除数之和后，变作一个平方数．例如：$7^3+(1+7+7^2)=20^2$．另一个问题是：要找出一个平方数，在加上其真除数之和后变作一个立方数．

第一个问题有一些解，见下表：

立方数	立方数的除数和＝一个平方数
$(3^3\cdot5\cdot11\cdot13\cdot41\cdot47)^3$	$(2^8\cdot3^2\cdot5\cdot7\cdot11\cdot13\cdot17\cdot29\cdot61)^2$
$(2\cdot3\cdot5\cdot13\cdot41\cdot47)^3$	$(2^7\cdot3^2\cdot5^2\cdot7\cdot13\cdot17\cdot29)^2$
$(17\cdot31\cdot47\cdot191)^3$	$(2^{10}\cdot3^2\cdot5\cdot13\cdot17\cdot29\cdot37)^2$
$(2^5\cdot5\cdot7\cdot31\cdot73\cdot241\cdot243\cdot467)^3$	$(2^{12}\cdot3^2\cdot5^3\cdot11\cdot13^2\cdot17\cdot37\cdot41\cdot113\cdot193\cdot257)^2$
$(3\cdot11\cdot31\cdot443\cdot499)^3$	$(2^9\cdot3\cdot5^4\cdot13\cdot37\cdot61\cdot157)^2$

表 2　除数和是平方数的某些特殊立方数

第二个问题的解如下：

平方数	平方数的除数和＝一个立方数
$(43098)^2=(2\cdot3\cdot11\cdot653)^2$	$(1729)^3=(7\cdot13\cdot19)^3$
$(2^2\cdot5\cdot7\cdot11\cdot37\cdot67\cdot163\cdot191\cdot263\cdot439\cdot499)^2$	$(3^2\cdot7^3\cdot13\cdot19\cdot31^2\cdot67\cdot109)^3$
$(7\cdot11\cdot29\cdot163\cdot191\cdot439)^2$	$(3\cdot7\cdot13\cdot19\cdot31\cdot67)^3$

表 3　除数和是立方数的某些特殊平方数

这类问题经常在几个数学小集团之间提来提去作为挑战．不同国家之间的数学家之间总是有很强烈的争奇斗胜思想．再

也没有什么东西能打动小集团成员的好胜心:——提出一套足以难倒对方的问题,而提出者却已掌握了它的一般解法.许多数学问题都由此而起,而最富有成果的数学发现也往往肇因于这种竞争.

类似的问题还有:试找出一个平方数,其除数之和也是平方数.或者:找出一个平方数,其真除数之和是一个平方数. [9]

一些实例见下表.

平方数	所有除数之和=一个平方数
$81=9^2$	$1+3+9+27+81=121=11^2$
$400=20^2$	$1+2+4+5+8+10+16+20+25+40+50+80+100+200+400=961=31^2$
$(3\cdot7\cdot11\cdot29\cdot37)^2$	$(3\cdot7\cdot13\cdot19\cdot67)^2$

表 4 某些特殊平方数,其除数和仍是平方数

平方数	真除数之和=一个平方数
$9=3^2$	$1+3=2^2$
$2401=49^2$	$1+7+49+343=400=20^2$

表 5 某些特殊平方数,其真除数之和为平方数

正整数的除数有着许多其他有趣规律.一个鲜为人知的性质是:如果数 N 有 p 个除数,则所有这些除数的乘积等于 $\sqrt{N^p}$.

参考文献

Barlow, P. *Theory of Numbers*. London: J. Johnson & Co., 1811.

Carmichael, R. D. *Theory of Numbers and Diophantine Analysis*. New York: Dover Publications, Inc., 1959.

Dickson, L. E. *History of the Theory of Numbers*. 3 vols. New York: Chelsea Publishing Co., 1950.

Escott, E. B. "Solution of Problem: Find a Number, x, Such

That the Sum of the Divisors of x Is a Perfect Square,"

[10] *American Mathematical Monthly*, **23**(1916),394.

第3章 完美无缺

人们一贯追求完美无缺，但后者老是巧妙地躲开他. 寻找“完全数”的努力已经历了许多世代，但找到的却是寥寥无几——到 1964 年为止，只找到 23 个[①]. 所谓完全数，就是真除数之和等于它的数，要求把一切除数相加起来，其中也包括数 1，但不包括此数本身. 绝大多数自然数是“富裕数”或“亏损数”，即它们的一切真除数之和超过或不到该数. 例如 24 的真除数之和为 36，而 15 的真除数之和为 9，等等. 6 是最小的完全数，它的真除数 1+2+3 加起来正好等于 6.

完全数极其稀少，而且它们之间相隔得很开；在 6 之后相继出现的完全数有 28；496；8128 以及 33550336. 迄今未发现过奇完全数. 6 与 28 曾被某些《圣经》注释家视为至高无上的建筑师——上帝的基本数字，其证据便是，世界万物是在 6 天之内创造完成的，而月亮的周期是 28 天[②].

同许多早期的希腊人与希伯来人一样，欧几里得(Euclid)曾研究过完全数. 他还知道偶完全数的公式. 欧几里得生活在 2300 多年以前. 从他那个时代以来已有大量辛勤劳动倾注于完全数的研究，而此领域仍然为研究者敞开着. 圣·奥古斯丁(St.

---

① 至 1996 年 11 月为止，共发现了 34 个完全数. ——译者注.

② 实际上朔望月的长度是 29.5306 日. 中国的阴历规定为大月 30 天、小月 29 天，都与 28 无关. 圣经注家的说法是属牵强附会. ——译者注.

Augustine)说过:"6是自身就完美的,这并不因为上帝在6天内创造了万物,毋宁说这句话的反面倒是真理;因为这个数很神圣,上帝才于6天内创造一切众生,即使6天的工作不存在,6仍然是完美无缺的."

尼可麦库斯(Nichomachus),在公元后100年左右很出名的一位数学家,有时也被认为是完全数28与496的发现人,曾经写道:"正像美丽与超群十分稀少,屈指可数;丑恶与伪劣却到处泛滥无序那样,富裕数与亏损数极为众多,它们的发现也是毫无章法.然而,完全数是屈指可数的,它们的出现也很井然有序."[11]

毕达哥拉斯(Pythagoras)(据认为他是著名定理"直角三角形两直角边的平方之和等于斜边的平方"的发现者)的追随者们认为完全数6是婚姻、健康、美丽的象征,因为它的组成部分是完整与和合的(参阅第18章).

公元12世纪的一个知名人士拉贝·约瑟夫·本·耶和达·安金(Rabbi Josef ben Jehuda Ankin)在其著作《灵魂的治疗》中曾介绍过完全数的研究.

在一本意大利文的著作里把完全数6归功于美神维纳斯,"它来自两性的结合,男方为3,是一个奇数;女方为2,是一个偶数."

欧几里得给出的偶完全数N的公式如下:

$$N=(2^{n-1})(2^n-1),\qquad\text{(公式 1)}$$

这里的n是一个大于1的正整数而能使第二个因子(2^n-1)为素数者.当$n=2,3,5,7,13$时这确实不错,可是不幸得很,以后的n却表现得毫无规律.与以上五个数值对应的便是上文已提到过的前五个完全数6;28;496;8128以及33550336.

这真是一桩怪事:欧几里得老早就知晓偶完全数公式,直到两千年以后大数学家欧拉(Euler)才证明欧几里得公式是偶完

全数唯一可能的公式.迄今仍然无人证明:奇数究竟能否是完全数.

如果真的存在着奇完全数 N,那么它与正常情况不一样,必须置于若干严厉的管制之下,这些条件简直使人感到迷茫,下面让我们仅仅给出其中的一些,让读者看看:

1. N 必须是一个用 12 去除时余数为 1,用 36 去除时余数为 9 的数.

2. 它至少要有六个不同的素数除数.

3. 它必须具有 $p^{4x+1}q_1^{2a_1}q_2^{2a_2}q_3^{2a_3}\cdots q_n^{2a_n}$ 的形式,这里,p 只能是 $4k+1$ 形式的素数,但 q 可为任意奇素数.

4. 此式还有进一步的限制:如果除了第一个以外,所有的 a 等于 1,则 a_1 不能等于 2;如果除了第一、第二个以外所有的 a 都等于 1,则前面两个(即 a_1,a_2)不能都等于 2.

5. 如果所有的 a 都等于 2,则 N 不可能是完全数.

6. 若所有的 q 的指数都递增 1,则由此得出的指数不能有 9,15,21 或 33 作为公共除数.

7. 若 p 的指数 $4x+1$ 等于 5,则所有的 a 都不能等于 1 或 2.

[12]

8. 若 N 不能被 3 整除,则它至少要有 9 个不同的素数除数;若 N 不能被 21 整除,则它至少得有 11 个这样的除数;若它不能被 15 整除,它至少要有 14 个不同的素数除数;若它不能被 105 整除,至少要有 27 个这样的除数,这将要求 N 至少大于 10^{44}.

9. 若 N 正好有 r 个不同素数除数,则最小的一个应小于 $r+1$.例如,若 N(假定它存在的话)有 28 个不同素数除数,则最小者不应大于 29.

对偶完全数$(2^{n-1})(2^n-1)$来说,存在的主要问题是:要找出一些 n 值,使$(2^{n-1})(2^n-1)$中第二个因子为一素数.W・W・R・鲍尔将 2^n-1 形式的数(n 为素数)称为“梅桑数”,因为法

国数学家梅桑(Mersenne)曾在1644年的著作《深入的看法》中对此种类型的数作过研究. 作为信息来源的梅桑猜想以及随之而起的广泛讨论在此项研究中形成一种强有力的刺激,促使人们付出大量计算代价来验证或否定梅桑的断言,然而此种努力并非全然白费,它也顺便带来了一些重要性质的发现. 而在目前,此种繁重工作基本上是由数字式计算机来承担的.

生活在17世纪的彼得·本果斯(Peter Bungus)是一群杂牌数学家中的一个,他们把数与无知奇怪地揉合在一起,很有点像炼金术士把化学与炼金术拼凑在一起那样,在一本名为《数的神秘》的书里头,他列出了24个数,据说它们全都是完全数,然而梅桑认为其中只有8个是说对的,即表6中所列出来的那几个. 接着,梅桑又添加了算在他自己名下的三个,即$n=67$;127;257,并声称它们给出了接在后面的完全数. 后世的研究家们指出梅桑所给出的值67与257是错误的,而他也遗漏了能得出素数的89与107. 从1644年到1947年,为了检查与改正梅桑的断言,竟然花费了303年!

n	完全数$(2^{n-1})(2^n-1)$	对应的梅桑数 $M_n=2^n-1$
2	6	3
3	28	7
5	496	31
7	8128	127
13	33550336	8191
17	8589869056	131071
19	137438691328	524287
31	2305843008139952128	2147483647

[13] 表6 完全数

梅桑是怎样得出他的结论来的?对此曾有过许多猜想,但经历三百余年以后没有找到什么结果. 说不定梅桑曾经发现或利用过一些定理,而这些定理后来失传了,没能重新再发现,看来

梅桑不太可能会使用经验性方法——要知道，$n=257$ 时，相应的梅桑数即已多达 78 位. 也有人认为才华横溢的数学家费马曾把这些结果通报给梅桑.

对于这样一个具有广泛魅力的问题，不可避免地会出现一些虚假新闻：有人声称发现了新的完全数. 在已经过去的几个世纪中，此种毫无基础的虚假消息时有所闻，这也不足为奇，因为彼得·本果斯厚颜无耻地给出的 24 个完全数，其正确率也只有三分之一. 然而 20 世纪还是不断出现一些索取名利之徒，犹如探险家被吸引到北极，数学家也被指数较大的梅桑数引诱，特别是 $n=257$ 的那一个.

1936 年 3 月 27 日，联合通讯社发了一个激动人心的报道"新完全数"，芝加哥的 S·I·克利格(Krieger)博士宣称他发现了一个 155 位的完全数 $2^{256}(2^{257}-1)$. 他认为，他已证明 $2^{257}-1$ 是个素数.《纽约先驱论坛报》上刊载的新闻报道如下：

有人宣称已发现 155 位的完全数

十足干了 5 年之久，终于证明了源自欧几里得的古老问题

芝加哥 3 月 26 日消息(联合通讯社)——今天，塞缪尔·I·克利格博士终于放下笔和纸，宣称他已解决了一个从欧几里得时代以迄于今挫败过无数数学家的大难题，他终于找到了一个十九位以上的完全数.

他解释道，所谓完全数，就是其真除数之和等于该数本身的数. 例如 28 是 1，2，4，7，14 之和，而后面的各数都能整除 28. 克利格博士的完全数有 155 位. 该数就是：26，815，615，859，885，194，199，148，049，996，411，692，254，958，731，641，184，786，755，447，122，

887,443,528,060,146,978,161,514,511,280,138,383,284,395,055,028,465,118,831,722,842,125,059,853,682,308,859,384,882,528,256.

[14] 它的算式是 2 的 513 次方减去 2 的 256 次方.

博士说他花费了 17 小时把它算了出来,但证明它却用了五年之久.

理应享有崇高荣誉的两位数论专家 M·克莱契克(M. Kraitchik)与 D·H·雷默(D. H. Lehmer)早已证明了 $2^{257}-1$ 是个合数,前者在 1922 年,后者在 1931 年.他们的方法尽管揭露了该数的本性,却没有透露其因子.究竟是谁的说法正确? 克利格博士还是克莱契克或者雷默?

后来,一些数学杂志狠狠地批评了报纸,他们只想耸人听闻,全然不顾准确性.报道消息里头提到的事,早就有四个完全数超过了 19 位,它们的位数分别有 37,54,65 与 77 位;其中 37 位的那一个完全数 $2^{60}(2^{61}-1)$,早在 1883 年即已发现.克利格博士过早地放下了他的笔,但疑团并未彻底消除,直到 1952 年美国国家标准局西部计算中心的 SWAC 电子计算机最终宣布 $2^{257}-1$ 的确是个合数为止.本书以后还要提到此事.

当 n 为合数时,2^n-1 恒为合数.因为若 n 为一个偶合数 $2y$,则表达式 2^n-1 便是平方差,它当然可以分解因式 $2^{2y}-1=(2^y+1)(2^y-1)$.例如:

$$(2^{14}-1)=(2^7+1)(2^7-1)=129\cdot 127=3\cdot 43\cdot 127.$$

若 n 是奇合数 $n=pq$,则有

$$\begin{aligned}2^{pq}-1&=(2^p)^q-1\\&=(2^p-1)[(2^p)^{q-1}+(2^p)^{q-2}+(2^p)^{q-3}+\\&\quad\cdots+(2^p+1)],\end{aligned}$$

这些都是代数教科书里讲过的内容. 例如:

$$2^{35}-1=(2^7)^5-1$$
$$=(2^7-1)[(2^7)^4+(2^7)^3+(2^7)^2+(2^7)+1]$$
$$=127\cdot 270549121.$$

由于它至少可以分解为两个因子之积,所以 $2^{35}-1$ 是个合数. 碰巧它的后一个因子也是合数,于是最终可分解为素因子乘积 $127\cdot 31\cdot 71\cdot 122921$.

尽管 n 为合数时 2^n-1 恒为合数,但当 n 为素数时,2^n-1 仍可能为合数. 在某些情况下可以利用某些定理,它们或者能直接分解出因子,或者可以为因子的个数设置一个合理的上界以供试探. 费马定理及其推论是用得最多的办法. [15]

这个大名鼎鼎的定理我们将在第 6 章中再次遇见,现在先让读者过一下目. 若 p 为素数而 a 不是 p 的倍数,则 $a^{p-1}-1$ 恒能被 p 整除. 例如 2^6-1 正好能被 7 整除. 也有可能若干比 $p-1$ 更小的指数 n 即能使 a^n-1 被 p 整除(例如 2^3-1 可以被 7 整除). 若 n 是此类指数中最小的一个,则它一定是 $p-1$ 的一个除数,换言之,$p-1$ 必等于 mn,于是 $p=mn+1$.

在形为 2^n-1 的梅森数中,指数 n 恒为素数,故一般可认为它是奇素数(除非 $n=2$,但这是极肤浅的). 由于费马定理中,p 亦为奇素数,于是 mn 一定是偶数,从而 m 亦必须是偶数,可把它记为 $2r$,于是 $p=2rn+1$. 这就给我们许多启迪,例如若 $2^{11}-1$ 有一奇除数 p(若它有任何除数的话,当然它有一个奇除数),则它必然具有 $2r\cdot 11+1=22r+1$ 的形式,而事实上当 $r=1$ 时,素数 23 真的能够整除 $2^{11}-1$. 与此类似,如果 $2^{17}-1$ 有一素除数,则它必然具有 $2r\cdot 17+1=34r+1$ 的形式. 但碰巧 $2^{17}-1$ 本身是个素数,所以唯一的此类形式的除数即是该数本身. 当 n 变得越来越大时,要进行试探的可能的除数,即使限定了某种形式,仍然是为数极大的,因此还得仰仗其他办法.

费马定理的改良形式可以对某些梅桑数的除数提供直接帮助.由此定理我们已经知晓，p 为素数时 $2^{p-1}-1$ 恒能被 p 整除.由于 p 是一个奇数，故 $p-1$ 为偶数，既然它能被 2 整除，所以是合数.可是在梅桑数中，所有的指数全是素数，于是从表面上看来，在寻找这些数的因子时，费马定理帮不了我们的忙.但有人已经作出证明[①]，对底数 2 来说，指数 $p-1$ 可除以 2 而不影响该数用 p 去除时的可除性，如 p 在除以 8 时余数为 1 或 7 的话，换言之，即其形式为 $8r+1$ 或 $8r+7$.从而可以推出

$$2^{[(8r+1)-1]/2}-1 \text{ 与 } 2^{[(8r+7)-1]/2}-1$$

可被各该形式的素数分别整除.在前一种情况，它告诉我们 $2^{4r}-1$ 能被形为 $8r+1$ 的素数整除，但由于指数 $4r$ 显然不是素数，所以这种数不属于梅桑数的类型.对后一种情况，我们的结论是 $2^{4r+3}-1$ 能被 $8r+7$ 形式的素数整除.所以，若 $4r+3$ 与 $8r+7$ 都是素数时，则 $8r+7$ 必能整除相应的梅桑数.

[16]

梅桑对他所研究的 2^n-1 形式的数，曾设置了一个上界，即 n 不超过 257；在此限制下，能满足上述两个条件的 r 与 n 的数值，可以参看附表 7.

r	$n=4r+3$，一个素数	$8r+7$ 是一个素数，从而是 2^n-1 的一个除数
2	11	23
5	23	47
20	83	167
32	131	263
44	179	359
47	191	383
59	239	479
62	251	503

表 7　梅桑数的除数

① 例如可参阅 Uspensky 与 Heaslet 合编的《初等数论》.——原注.

已经研究出一些非常巧妙的办法来大大削减试探的工作量，其中也包括我们将在本书第21章中将要提到的光电析因子机器. 在寻找很大的完全数时，现代数字电子计算机极为有效，它们能在数秒钟内完成数以年计的手算工作量.

法国数学家E・V・卢卡发明了一种测试法来检查梅桑数的素性. D・H・雷默对此作了改进，使之十分有效、实用，以致他同别的研究者可用来核查以前未能分辨清楚的许多梅桑数的素性. 经过雷默改进后的卢卡测试法需要利用数列：

$$4;\ 14;\ 194;\ 37634;\ \cdots;\ u_n=u_{n-1}^2-2,$$

其中每一项是前一项的平方减2. 当且仅当此数列的第$(n-1)$项能被$N=2^n-1$整除时，N才是素数；否则，它就是合数. 例如37634是数列的第四项，若$2^5-1=31$能整除它，则31就是素数. 而情况确是如此. 不幸的是，数列的项递增得极快，因此对很大的n值来说，测试变得不切实用，除非这种“不能动摇的东西”遇到了“无法抵挡的力量”——现代数字式计算机. 美国国家标准局西方计算中心的SWAC计算机在1953年被指定要承担这项工作. 要把卢卡法则调节到计算机的性能范围需要利用184条分散指令. 对应于$n=521;607;1279;2203;2281$的五个完全数是通过SWAC计算机发现的. D・H・雷默博士，这位曾在梅桑数上花费许多时光的学者，亲眼看到电子计算机在短短48秒钟内做完了他20年前用一台计算机花去700多小时才完成的艰辛劳动，最后证明$2^{257}-1$的确是一个合数. 梅桑曾经说过，要判定一个15或20位数字是否素数，千生万世都是远远不够的. 但是在寥寥数小时内，SWAC就检查了42个数，其中最小的一个有80位. 它一共只用了$13\frac{1}{2}$分钟即已判明$2^{1279}-1$是个素数. 若不是计算机而由人来干这件事情，那就要花费125年时间. 想作出什么预测，那简直是蠢事. 尽管如此，人的辛勤劳动依然不能低估. H・S・乌勒(Uhler)仅仅使用了一架台式计算机，

[17]

就发现了 6 个梅桑数都是合数，即 $n=157;167;193;199;227$ 与 229.

雷默博士说，在 p 为素数时要测试一个梅桑数 M_p 是否为素数，计算机大致要用去 $\left(\frac{p}{100}\right)^3$ 秒. 一般地说，SWAC 的一分钟相当于一个人用台式计算机整整工作一年.

在表 8 中，给出了在梅桑上限 257 以内的 12 个完全数，此外还得加上紧随于其后的，n 在257与11213之间的11个完全数.

在限度 257 以内，梅桑数 $M_n=2^n-1$ 的因子状况，作者所掌握的最近信息如下：对 $n=2,3,5,7,13,17,19,31,61,89,107,127$ 这十二个值而言，相应的梅桑数是素数；对 $n=11,23,29,37,41,43,47,53,59,67,71,73,79,83,97,103,113,151,163,179,181$ 来说，相应的梅桑数是合数且已完成全部因子分解；对 $n=173,191,223,229,233,239,251$ 而言，相应的梅桑数是合数，且已知两个或更多因子；对 $n=109,131,157,167,193,197,211,241$ 来说，此类梅桑数为合数，但只知道它的一个因子；对 $n=101,137,139,149,199,227$ 与 257 而言，仅仅知道相应的梅桑数为合数，但连一个因子都未能求出. 不过，在 $n=101$ 时，这个梅桑数只有两个素因子. 表 9 给出了至少已知其一个因子的合数梅桑数. 已知为合数但连一个因子都未能求出的 7 个梅桑数中的 6 个在表中未予列入，然而 $n=101$ 的情况已被收入此表.

表 8 显示了梅桑素数分布的不规则性. 在 2 与 127 之间（包括首尾两个素数）共有31个素数，其中梅桑素数有12个；[18] 但在其下一段131至521之间共有66个素数，梅桑素数却连一个都没有. $2^{127}-1$ 与 $2^{257}-1$ 之间的所有 24 个梅桑数统统都是合数，还得加上 $2^{257}-1$ 至 $2^{521}-1$ 之间的 42 个梅桑合数. 在 521 到 607 间只有 12 个素数，其相应的梅桑数 M_n 全是合数. 其后的 607至1279之间有95个素数，接着又要经过长长的、120个

素数 n	梅桑数 $M_n=(2^n-1)$是素数	位数	完全数$(2^{n-1})(2^n-1)$		位数
2	3	1	$2^1(2^2-1)$ =	6	1
3	7	1	$2^2(2^3-1)$ =	28	2
5	31	2	$2^4(2^5-1)$ =	496	3
7	127	3	$2^6(2^7-1)$ =	8128	4
13	8191	4	$2^{12}(2^{13}-1)$ =	33550336	8
17	131071	6	$2^{16}(2^{17}-1)$ =	8589869056	10
19	524287	6	$2^{18}(2^{19}-1)$ =	137438691328	12
31	2147483647	10	$2^{30}(2^{31}-1)$ =	2305843008139952128	19
61	2305843009213693951	19	$2^{60}(2^{61}-1)$		37
89	618970019642690137449562111	27	$2^{88}(2^{89}-1)$		54
107	$2^{107}-1$	33	$2^{106}(2^{107}-1)$		65
127	$2^{127}-1$	39	$2^{126}(2^{127}-1)$		77
521	$2^{521}-1$	157	$2^{520}(2^{521}-1)$		314
607	$2^{607}-1$	183	$2^{606}(2^{607}-1)$		366
1279	$2^{1279}-1$	386	$2^{1278}(2^{1279}-1)$		770
2203	$2^{2203}-1$	664	$2^{2202}(2^{2203}-1)$		1327
2281	$2^{2281}-1$	687	$2^{2280}(2^{2281}-1)$		1373
3217	$2^{3217}-1$	969	$2^{3216}(2^{3217}-1)$		1937
4253	$2^{4253}-1$	1281	$2^{4252}(2^{4253}-1)$		2561
4423	$2^{4423}-1$	1332	$2^{4422}(2^{4423}-1)$		2663
9689	$2^{9689}-1$	2917	$2^{9688}(2^{9689}-1)$		5834
9941	$2^{9941}-1$	2993	$2^{9940}(2^{9941}-1)$		5985
11213	$2^{11213}-1$	3376	$2^{11212}(2^{11213}-1)$		6751

表 8　完全数与梅桑数

素数的间隔，才能得到素数 $2^{2203}-1$. 可是 2203 至 2281 间仅有 10 个素数，倒又有一个梅桑素数出现了. 接着，又是一个长长的，116 个素数的间隔才出现第 18 个完全数所对应的指数 $n=3217$. 表 8 中最后 5 个梅桑素数的间隔是 128；19；594；30 与 131 个素数.

某些读者也许想知道偶完全数公式是怎样推导出来的. 第 2 章中我们已给出一个数：

$$N = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

的除数个数，而数 N 的各个除数之和则由下列公式

$$\frac{p_1^{a_1+1}-1}{p_1-1} \cdot \frac{p_2^{a_2+1}-1}{p_2-1} \cdots \frac{p_n^{a_n+1}-1}{p_n-1} \qquad (\text{公式 } 2)$$

给出. 例如，若 $N=240$，我们先把它表示为质因数的连乘积 $2^4 \cdot 3 \cdot 5$，然后 N 的各个除数之和(通常记为 N 的函数 $S(N)$)等于

$$\frac{2^{4+1}-1}{2-1} \cdot \frac{3^{1+1}-1}{3-1} \cdot \frac{5^{1+1}-1}{5-1} = 31 \cdot 4 \cdot 6 = 744.$$

在此和数中，数本身也被看作一个除数而包括进去了.

现在我们准备导出完全数公式. 设有一个偶完全数 $N=2^a q$，这里 q 表示所有奇素数乘幂之积. 我们将要证明 q 实际上只是一个素数而且具有特殊形式. 为了方便起见，我们无需写出像公式 2 那样的复杂表达式，设 s 是 q 的一切除数(其中也包括 q 本身在内)之和，而 d 只是它的真除数之和，于是 $s=q+d$.

由公式 2 可知，2^a 的一切除数之和为 $(2^{a+1}-1)/(2-1)=2^{a+1}-1$. 因此 N 的全部除数之和等于 $(2^{a+1}-1)\cdot s$，在完全数的场合，这个和数应是数 N 的二倍，因为前已说过，公式 2 中包括了该数本身在内. 于是我们就得出 $2N$ 或 $2(2^a q)$，即 $2^{a+1}q=(2^{a+1}-1)\cdot s$，亦即 $(2^{a+1}-1)(q+d)$. [20]

化简后，即得出

素数 n	梅桑数 2^n-1 的因子
11	2047=23 · 89 C[①]
23	8388607=47 · 178481 C
29	536870911=233 · 1103 · 2089 C
37	137438953471=223 · 616318177 C
41	2199023255551=13367 · 164511353 C
43	8796093022207=431 · 9719 · 2099863 C
47	2351 · 4513 · 13264529 C
53	6361 · 69431 · 20394401 C
59	179951 · 3203431780337 C
67	193707721 · 761838257287 C
71	228479 · 48544121 · 212885833 C
73	439 · 2298041 · 9361973132609 C
79	2687 · 202029703 · 1113491139767 C
83	167 · 57912614113275649087721 C
97	11447 · 13842607235828485645766393 C
101	素数 · 素数 C
109	745988807 · ?
113	3391 · 23279 · 65993 · 1868569 · 1066818132868207 C
131	263 · ?
151	18121 · 55871 · 165799 · 2332951 · 7289088383388253664437433 C
157	852133201 · ?
163	150287 · 704161 · 110211473 · ?
167	2349023 · ?
173	730753 · 1505447 · ?
179	359 · 1433 · ?
181	43441 · 1164193 · 7648337 · ?
191	383 · ?
193	13821503 · ?
197	7487 · ?
211	15193 · ?
223	18287 · 196687 · 1466449 · 2916841 · ?
229	1504073 · 20492753 · ?
233	1399 · 135607 · 622577 · ?
239	479 · 1913 · 5737 · 176383 · 134000609 · ?
241	22000409 · ?
251	503 · 54217 · ?

表 9　梅桑数的因子　[21]

$$2^{n+1}-1=q/d.$$

这意味着 d 是 q 的一个真除数，如前给出之定义，它也等于

① 记号 C 表示此数已被完全分解；它的所有素因子均已求出．对 $n=101$ 来说，只知两个因子均为素数，但未能求出．——原注．

q 的真除数之和，因而 d 只能是 q 的唯一真除数，于是 d 的唯一可能值是 1. 然而，若一数的真除数之和为 1，则该数必然是一个素数.

因此，$q=2^{a+1}-1$ 是个素数；由于 N 等于 $2^a q$，所以它就是 $2^a(2^{a+1}-1)$. 如果令 $a+1=n$，它就完全同公式 1 吻合. 证明完毕.

* * *

除去第一个完全数 6(此时相当于 $a=1$)之外，任一偶完全数 $2^a(2^{a+1}-1)$ 是前 $2^{\frac{a}{2}}$ 个奇数的立方和. 例如，$a=2$ 时，完全数 $28=1^3+3^3$；$a=4$ 时，完全数 $496=1^3+3^3+5^3+7^3$；$a=6$ 时，完全数 $8128=1^3+3^3+5^3+7^3+9^3+11^3+13^3+15^3$ 等等. 立方数与完全数之间居然有如此奇妙联系，这是出乎人们意料之外的.

* * *

数学家们并不满足于普通完全数，他们又进一步发现了多重完全数——某数的一切除数之和是该数的一个倍数. 通常的完全数称为 P_2，因为它们的各除数之和等于原数的二倍. P_3 则意味着除数之和为原数的三倍，如此等等. 作为 P_3 的一个实例是数 120，它的一切除数之和 $1+2+3+4+5+6+8+10+12+15+20+24+30+40+60+120$ 等于 360，即 120 的 3 倍. 下面的附表中给出了多重完全数的其他一些例子.

重度	完全数
3	672
4	30240
4	$2^{41}\cdot3^{12}\cdot7^4\cdot11^2\cdot13^4\cdot17^2\cdot19^2\cdot43\cdot103\cdot127\cdot151\cdot191\cdot271\cdot307\cdot337\cdot467\cdot617\cdot911\cdot2801\cdot5419\cdot30941\cdot398581\cdot797161$
5	14182439040
6	$2^{23}\cdot3^7\cdot5^3\cdot7^4\cdot11^3\cdot13^3\cdot17^2\cdot31\cdot41\cdot61\cdot241\cdot307\cdot467\cdot2801$
7	$2^{46}\cdot3^{15}\cdot5^3\cdot7^5\cdot11\cdot13\cdot17\cdot19^4\cdot23\cdot31\cdot37\cdot41\cdot43\cdot61\cdot89\cdot97\cdot151\cdot193\cdot911\cdot2351\cdot4513\cdot442151\cdot13264529$

[22]

表 10 多重完全数

有时,一数的真除数之积(而不是其和)有可能等于该数的某个乘幂,如表 11 所示.

数 N	$\pi(d)=N$ 的真除数乘积	
12	$1\cdot2\cdot3\cdot4\cdot6=$	$144=12^2$
20	$1\cdot2\cdot4\cdot5\cdot10=$	$400=20^2$
45	$1\cdot3\cdot5\cdot9\cdot15=$	$1225=45^2$
24	$1\cdot2\cdot3\cdot4\cdot6\cdot8\cdot12=$	$13824=24^3$
40	$1\cdot2\cdot4\cdot5\cdot8\cdot10\cdot20=$	$64000=40^3$
48	$1\cdot2\cdot3\cdot4\cdot6\cdot8\cdot12\cdot16\cdot24=$	$5308416=48^4$
80	$1\cdot2\cdot4\cdot5\cdot8\cdot10\cdot16\cdot20\cdot40=$	$40960000=80^4$
405	$1\cdot3\cdot5\cdot9\cdot15\cdot27\cdot45\cdot81\cdot135=$	$26904200625=405^4$

表 11 一数的真除数乘积等于此数的某个乘幂

除了完全数之外,数 $2^n\pm1$ 本身也经常被人们研究. 对许多很大的 n 值,此类数字已被部分或完全分解. 美国陆军武器装备电子数字积分计算机 ENIAC 曾被用来计算这些数的因子,并曾用于研究满足关系式 $2^n\equiv2 \bmod n$的合数 n,分解它们的素数因子. 实际例子有 $n=100463443$, $p=7577$; 以及 $n=199674721$,$p=4261$.

满足同余式 $2^m-2\equiv0 \bmod m$的偶数 m 极其稀少,其中的一例是 $161038=2\cdot73\cdot1103$,另外三个数是 215326,2568226 与 143742226.

参 考 文 献

Archibald, R. C. "Mersenne's Numbers," *Scripta Mathematica*, **3**(1935),112.

Associated Press. "Perfection Is Claimed for 155-Digit Number," *New York Herald Tribune*,**95**(March 27,1936),21.

Ball W. W. R. *A Short Account of the History of Mathematics*. New York: Dover Publications, Inc. ,1960.

——. *Mathematical Recreations and Essays*. New York:

Macmillan Co. ,1939.

Barker, C. B. "Proof That the Mersenne Number M_{167} Is Composite," *Bulletin of the American Mathematical Society*, **51**(1945),388.

Barlow, P. *Theory of Numbers*. London: J. Johnson & Co. , 1811.

Beeger, N. G. W. H. "On Even Numbers m Dividing 2^m-2," *American Mathematical Monthly*, **58**(1951),553. [23]

Bell, E. T. *The Last Problem*. New York: Simon and Schuster, 1961.

Bickmore, C. E. "On the Numerical Factors of a^n-1," *Messenger of Mathematics*, **25**(1895),1.

Brauer, A. "On the Non-Existence of Odd Perfect Numbers of the Form $p^a q_1^2 q_2^2 \cdots q_{t-1}^2 q_t^4$," *Bulletin of the American Mathematical Society*, **49**(1943),712.

Brillhart, J. , and Johnson, G. D. "On the Factors of Certain Mersenne Numbers," *Mathematics of Computation*, **14** (1960),365.

Carmichael, R. D. *Theory of Numbers and Diophantine Analysis*. New York: Dover Publications, Inc. , 1959.

——. "A Table of Multiply-Perfect Numbers," *Bulletin of the American Mathematical Society*, **13**(1907),383.

Carmichael, R. D. , and Mason, T. E. "Note on Multiply-Perfect Numbers. . . ," *Proceedings of the Indiana Academy of Science*(1911),257.

Dantzig, T. *Number: The Language of Science*. New York: Macmillan Co. ,1954.

Dickson, L. E. *History of the Theory of Numbers*. 3 vols. New York: Chelsea Publishing Co. , 1950.

Franque, B., and Garcia, M. "Some New Multiply-Perfect Numbers," *American Mathematical Monthly*, **60** (1953), 459.

Gillies, D. B. "Computer Discovers New Prime Number," *Science News Letter*, **83**(May 11, 1963), 291.

Hurwitz, A. "New Mersenne Primes," *Mathematics of Computation*, **16**(1962), 249.

Kraitchik, M. "On the Factorization of $2^n \pm 1$," *Scripta Mathematica*, **18**(1952), 39.

Lehmer, D. H. "On the Converse of Fermat's Theorem," *American Mathematical Monthly*, **43**(1936), 347.

——. "Factor Tables for the First Ten Million," *American Mathematical Monthly*, **56**(1949), 103.

——. "Test for Primality by the Converse of Fermat's Theorem," *Bulletin of the American Mathematical Society*, **33** (1927), 327.

——. "A Further Note on the Converse of Fermat's Theorem," *Bulletin of the American Mathematical Society*, **34** (1928), 54.

——. "Note on Mersenne Numbers," *Bulletin of the American Mathematical Society*, **38**(1932), 383.

——. "Some New Factorizations of $2^n \pm 1$," *Bulletin of the American Mathematical Society*, **39**(1933), 105.

——. "On the Factors of $2^n \pm 1$," *Bulletin of the American Mathematical Society*, **53**(1947), 164.

——. "On Lucas's Test for the Primality of Mersenne's Numbers," *Journal of the London Mathematical Society*, **10** (1935), 162.

Licks, H. E. *Recreations in Mathematics*. New York: D. Van

Nostrand Co. , 1921.

National Bureau of Standards. "National Bureau of Standards' Western Automatic Computer," *Technical News Bulletin*, [24] **37**(Oct. ,1953),145.

Powers, R. E. "The Tenth Perfect Number," *American Mathematical Monthly*, **18**(1911),195.

——. "Note on a Mersenne Number," *Bulletin of the American Mathematical Society*, **40**(1934),883.

Reid, C. "Perfect Numbers," *Scientific American*, **188** (March, 1953),84.

Riesel, H. "Mersenne Numbers," *Mathematical Tables and Other Aids to Computation*, **12**(1958),207.

——. "All Factors $q<10^8$ in All Mersenne Numbers, $2^p-1, p$ a Prime $<10^4$," *Mathematics of Computation*, **16** (1962), 478.

Touchard, J. "On Prime Numbers and Perfect Numbers," *Scripta Mathematica*, **19**(1953),35.

Uhler, H. S. "Note on the Mersenne Numbers M_{157} and M_{167}," *Bulletin of the American Mathematical Society*, **52** (1946),178.

——. "On Mersenne's Number M_{199} and Lucas's Sequences," *Bulletin of the American Mathematical Society*, **53**(1947), 162.

——. "On Mersenne's Number M_{227} and Cognate Data," *Bulletin of the American Mathematical Society*, **54**(1948),378.

——. "A Brief History of the Investigation of Mersenne Numbers and the Latest Immense Pairs," *Scripta Mathematica*, **18**(1952),122.

——. "Full Values of the First Seventeen Perfect Numbers,"

Scripta Mathematica, **20**(1954), 240.

Uspensky, J. V., and Heaslet, M. A. *Elementary Number Theory*. New York: McGraw-Hill Book Co., 1939.

Van Der Pol, B. "Radio Technology and Theory of Numbers," *Journal of the Franklin Institute*, **255**(1953), 476.

——. "Addendum and Correction to 'Radio Technology and Theory of Numbers,'" *Journal of the Franklin Institute*, **256**(1953), 265.

Woodall, H. J. "Mersenne's Numbers," *Manchester Literary and Philosophical Society, Memoirs and Proceedings*, **56** (1911—1912), 1. [25]

第4章 亲如手足

你想在圣·瓦伦丁节[①]向亲密的异性朋友表达深情厚意吗？那就请你利用数论知识.送一张贺卡，上面写点东西，譬如说：

约翰——1184

玛丽——1210

或者在致贺者的姓名处打上一个问号“?”.随后，你可向对方解释，1184与1210是一对“亲和数”.为了令人信服，或许你也可以利用6或其他完全数以作为吉祥物，象征你们互相幸福以及两性的完美结合.1184与1210之所以称为“亲和数”，是因为它们具有一个特性：这对数字中，一个数的所有真约数之和正好等于另一数.例如：

$$1+2+4+8+16+32+37+74+148+296+592=1210,$$

$$1+2+5+10+11+22+55+110+121+242+605=1184.$$

正如人们所料，我们的偏爱神秘主义的祖先对于上述爱情附加物有着各种不同解释.在《圣经·创世纪》的32节14款中，耶各的礼物200只母山羊与20只公山羊，被《圣经》的一位注释者说成是一种有意的秘密安排，因为220是亲和数对220，284

① 即每年的阳历2月14日，通称“情人节”.在本世纪的几个“闰八月”的年头(如1976，1995等年份)，这一天正好与元宵节(阴历正月十五日)重合.——译者注.

中的一个，耶各想用这种办法赢得埃索的友谊. 毕达哥拉斯说过一句名言："密友就是另一个自我，如同 220 与 284 一样."

11 世纪的一位阿拉伯人埃尔·马德施利蒂（El Madschriti）曾测试过这些数字的情欲效应，他让别人吃较小的数 220，自己吃较大的. 此种行径对堕入情网的现代人或许是一种很有价值的提示，他可以请情人享用嵌着一个亲和数的糕饼或糖果，与此同时，他自己则津津有味地吃着另一只. 如想取得更好的效果，那就尽可以先吃后解释. [26]

尽管早在《圣经》时代，人们就已表现出对亲和数的很大兴趣，然而这些数字的生成规律则仍有待于澄清. 1750 年，数学大师欧拉正确地列出了 60 对亲和数，可是他遗漏了第二个最小的一对 1184 与 1210，后者迟至 1866 年才被一位年仅 16 岁的少年巴格尼尼（B. N. I. Paganini）发现，所有生活在那个成果涌现的世纪中的专家都未能发现这对亲和数.

与生成完全数只有单一公式不同，有好多种方法可以产生亲和数. 下面讲一种来自阿拉伯数学家塔别特·本·考拉（Thabit ben Korrah）的办法：

取 2 的任意次幂 2^x，此处 $x>1$，并形成下列各数：

$$a=3\cdot 2^x-1,$$
$$b=3\cdot 2^{x-1}-1,$$
$$c=9\cdot 2^{2x-1}-1.$$

如它们都是素数，则 2^xab 与 2^xc 便是一对亲和数. 当 $x=2$ 时，由此即可给出数 220 与 284. 下面的附表 12 将给出另外几对.

2620	5020	6232	10744	17296
2924	5564	6368	10856	18416

9363584	111448537712
9437056	118853793424

表 12 一些亲和数对

人们必然要问这样一个问题：把某数的一切真约数相加，得出一个结果，如果再把作为其结果的数的真约数相加，如此反复进行，将会出现什么情况？譬如说，20 的真约数之和是 1+2+4+5+10=22，而 22 的真约数之和为 1+2+11=14，14 的真约数之和是 1+2+7=10，而 10 的真约数之和 1+2+5=8，8 的真约数之和等于7，最后我们发现7的真约数只有1. 大多数情况正是如此下场. 但也有真约数之和越变越大，无限递增的情[27]况.

有时也会出现循环反复，即某些真约数之和又回复到以前曾经出现过的情况，这时，我们将称之为“高阶亲和数”，或者也可用一个新名词“社交数”. 显然，如果通过一次相加即可返回原数，这是完全数的情况；通过两次相加，我们得到的是一般亲和数，这是因为数 n 的真约数之和等于 m，而后者的真约数之和等于 n. 数学家们用记号 $s(n)$ 表示数 n 的真约数之和. 为了紧凑，他们不写 $s[s(n)]$，而直接写成 $s^2(n)$. 这当然决不意味着 s 的平方去乘上 n，而是两次真约数相加. 由此可知，在完全数的场合有 $s(n)=n$，而在一般亲和数的场合有 $s^2(n)=n$. 继续进行下去的话，$s^k(n)=n$ 称为 k 阶亲和数，它将包含一个 k 数循环，而首尾均是数 n，而 k 个相应的和数则全都是 k 阶亲和数.

数 12496 即是一个实例，它的 $s(n)=14288$；$s^2(n)=15472$；$s^3(n)=14536$；$s^4(n)=14264$；$s^5(n)=12496=n$，原数又回来了. 真正令人惊讶的数是 14316，它竟然是具有 28 节的长链，即是说 $s^{28}(14316)=14316$. 也许读者在查阅附表 14 与图 1 之前愿意自己去验证一番.

正如著名的三个火枪手①，也存在着所谓“亲和三数组”，此数组中的任何一数，其真约数之和等于其他两数之和，附表 13 给出了两个实例.

① 法国名作家大仲马同名小说中的主要角色. ——译者注.

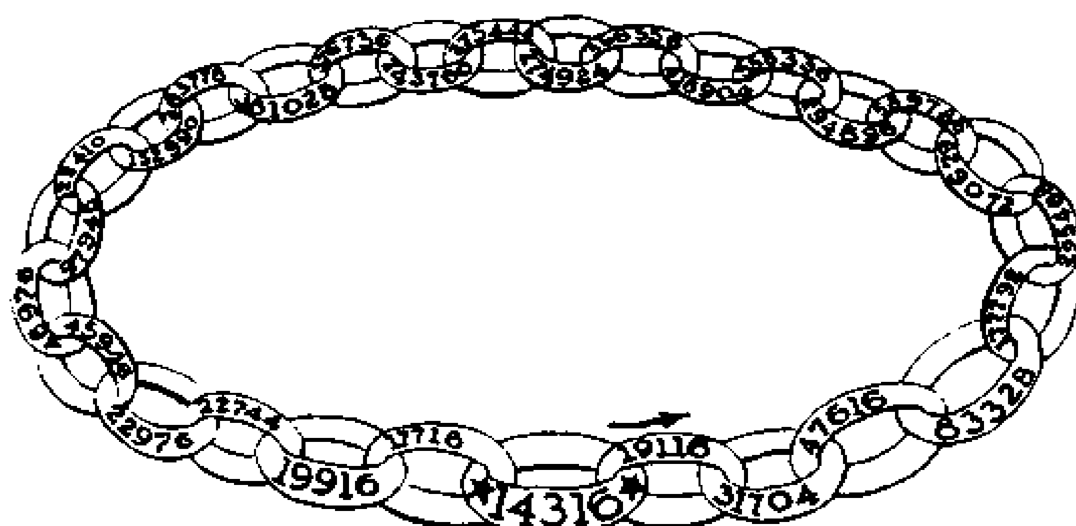


图 1 奇妙的 28 节亲和数长链 [28]

$2^{14}\cdot3\cdot5\cdot19\cdot31\cdot89\cdot151$	$2^{5}\cdot3\cdot13\cdot293\cdot337$
$2^{14}\cdot5\cdot11\cdot19\cdot29\cdot31\cdot151$	$2^{5}\cdot3\cdot5\cdot13\cdot16561$
$2^{14}\cdot5\cdot19\cdot31\cdot151\cdot359$	$2^{5}\cdot3\cdot13\cdot99371$

表 13 亲和三数组

序号	各节所代表之数 整数形式	各节所代表之数 质因数连乘积形式	真约数的个数
1	14316	$2^{2}\cdot3\cdot1193$	11
2	19116	$2^{2}\cdot3^{4}\cdot59$	29
3	31704	$2^{3}\cdot3\cdot1321$	15
4	47616	$2^{9}\cdot3\cdot31$	39
5	83328	$2^{7}\cdot3\cdot7\cdot31$	63
6	177792	$2^{7}\cdot3\cdot463$	31
7	295488	$2^{6}\cdot3^{5}\cdot19$	83
8	629072	$2^{4}\cdot39317$	9
9	589786	$2\cdot294893$	3
10	294896	$2^{4}\cdot7\cdot2633$	19
11	358336	$2^{6}\cdot11\cdot509$	27
12	418904	$2^{3}\cdot52363$	7
13	366556	$2^{2}\cdot91639$	5

表 14 有 28 节的亲和数链

（每一节所表示之数，其真约数之和等于下一节所代表的数）

序号	整数形式	质因数连乘积形式	真约数的个数
	各节所代表之数		
14	274924	$2^2 \cdot 13 \cdot 17 \cdot 311$	23
15	275444	$2^7 \cdot 13 \cdot 5297$	11
16	243760	$2^4 \cdot 5 \cdot 11 \cdot 277$	39
17	376736	$2^5 \cdot 61 \cdot 193$	23
18	381028	$2^2 \cdot 95257$	5
19	285778	$2 \cdot 43 \cdot 3323$	7
20	152990	$2 \cdot 5 \cdot 15299$	7
21	122410	$2 \cdot 5 \cdot 12241$	7
22	97946	$2 \cdot 48973$	3
23	48976	$2^4 \cdot 3061$	9
24	45946	$2 \cdot 22973$	3
25	22976	$2^6 \cdot 359$	13
26	22744	$2^3 \cdot 2843$	7
27	19916	$2^2 \cdot 13 \cdot 383$	11
28	17716	$2^2 \cdot 43 \cdot 103$	11
29	14316	$2^2 \cdot 3 \cdot 1193$	11

表 14 有 28 节的亲和数链(续)

[29] (每一节所表示之数,其真约数之和等于下一节所代表的数)

参 考 文 献

Barlow, P. *Theory of Numbers.* London: J. Johnson & Co., 1811.

Dickson, L. E. *History of the Theory of Numbers.* 3 vols. New York: Chelsea Publishing Co., 1950.

Ozanam, J. *Recreations in Science and Natural Philosophy.* [30] London: T. Tegg, 1884.

第5章 大师的发明

下面的戏法很有效，可多次重复. 请人家挑一个小于1000的正整数，相继用7，11，13去除它，并告诉你三个余数是什么. 这时你就能指出他原先选定的数. 做到这一点其实不难，你只需把三个余数分别乘以"魔数"715，364，924，把所得的积相加，再从结果中尽量减去1001的整数倍，以留下一个正整数的剩余，而此剩余即为他选定的数. 例如，若余数是5，6，3，便得

$$\begin{aligned} 715 \cdot 5 &= 3575 \\ 364 \cdot 6 &= 2184 \\ 924 \cdot 3 &= \underline{2772} \\ & \quad 8531 \end{aligned}$$

1001的倍数，首尾具有同样数码，例如2002，16016，35035等等. 对本例而言，要减去8008，即含于8531中的、1001的最大整倍数. 剩余数是523，即原先选定之数.

在作出解释之前，有必要学点同余知识，它是号称"数学王子"的卡尔·弗里德列希·高斯(Karl Friedrich Gauss)的精致发明. 在数论里头，我们时常要测试一数 n 能否为另一数 m 整除. 此时，商数显得并不重要，我们感兴趣的仅仅是余数以及使之为0的条件. 高斯为之发明了一种非常紧凑而高度有效的记号. 不考虑无关因素，我们得出了有关整数与可除性的全新且熠熠发光的概念. 就通常的算术而言，如果我们用13去除31，则一般记作

$$\frac{31}{13}=2+\frac{5}{13}.$$

[31] 试拿它与 $31\equiv 5 \mod 13$ 作对比，后一式读作“31 与 5 同余，模 13”，其意思是，31 被除数（即模）13 去除时，余数为 5.

作了这样的安排之后，同余式就很像方程，我们可对之作许多运算. 例如，可在其两边同时加 3，得到

$$34\equiv 8 \mod 13.$$

也可在两边同时减 5，得

$$26\equiv 0 \mod 13.$$

可在其两边同时乘上 2，即

$$62\equiv 10 \mod 13.$$

如乘以 4，则将有

$$124\equiv 20 \mod 13.$$

但由于

$$20\equiv 7 \mod 13,$$

所以可记为

$$124\equiv 7 \mod 13.$$

另外，原同余式两边各自平方，得

$$31^2\equiv 5^2\equiv 12 \mod 13,$$

由于 12 在除以 13 时缺少一个单位，故亦可记作

$$31^2\equiv 5^2\equiv 12\equiv -1,$$

那便是负的余数.

同余式的运算法则并不是同方程完全一样，在同余式的两

边同除以一数时尤需注意.例如,尽管有 $16\equiv1 \mod 5$,但通常并不能写作 $8\equiv\frac{1}{2} \mod 5$.(但最近同余式概念已可推广到分数范围.)另外,即便有 $40\equiv10 \mod 15$,我们也不能得出关系式 $4\equiv1 \mod 15$.仅当除数与模互质时,我们才能用它去除同余式的两边,否则,模也应被这个公因子去除,所以 $4\equiv1 \mod 3$.

此种方法在处理乘幂时开始显示出威力(不仅是双关语①). [32]

证明 $97^{104}-1$ 恰能为 105 整除,即

$$97^{104}\equiv 1 \mod 105 = 3\cdot5\cdot7,$$

我们可如下进行:

$$97\equiv1 \mod 3,\text{从而 } 97^{104}\equiv1^{104}\equiv1 \mod 3.$$

另有

$$97\equiv2 \mod 5,$$

$$97^2\equiv2^2\equiv4\equiv-1 \mod 5.$$

负剩余也是允许的.

$$97^4\equiv(-1)^2\equiv1 \mod 5,$$

于是有

$$(97^4)^{26}\equiv97^{104}\equiv1^{26}\equiv1 \mod 5.$$

最后,

$$97\equiv-1 \mod 7,$$

$$97^{104}\equiv(-1)^{104}\equiv1 \mod 7.$$

把以上三式结合起来,由于没有公因子,其中之一的可除性当然不影响另外两者的可除性,于是得出:

---

① 按原文 power 一词,既有"威力"的意思,在数学中又可解作"乘幂".——译者注.

$$97^{104} \equiv 1 \bmod 3 \cdot 5 \cdot 7 = 105,$$

由此可见，只要你用惯了它，方法其实是相当容易的.

现在要证明

$$2^{12} \equiv 1 \bmod 13.$$

曾经一度有过错误的猜想，即 $2^{2^x}+1$ 形式的数必是素数. 实际上，x 取 5 是一个最小的反例，由此即得出合数，它能为 641 整除. 很容易用同余式加以证明.

即我们需证出

$$2^{32} + 1 \equiv 0 \bmod 641,$$

或
$$2^{32} \equiv -1 \bmod 641.$$

开始时可选择一个 2 的乘幂，使之尽量接近于模，如果不是靠得很近的话，那就接近于模的倍数. 就本例而言，$3 \times 641 = 1923$ 很接近于 2^{11}，即 2048，而差数 125 的本身又恰为一个乘幂，带来了出乎意外的方便. 从而有

[33]
$$2^{11} \equiv 125 \equiv 5^3 \bmod 641.$$

于是

$$2^{22} \equiv 5^6 = 5^4 \cdot 5^2 \equiv -2^4 \cdot 5^2.$$

因当除数与模互质时，可用该数去除同余式的两边，所以我们可用 2 去除，于是得出：

$$2^{21} \equiv -2^3 \cdot 5^2,$$

再将此结果与 $2^{11} \equiv 5^3$ 相乘，便有

$$2^{32} \equiv -2^3 \cdot 5^5 = -2^3 \cdot 5 \cdot 5^4 \equiv -40(-16) = 640 \equiv -1.$$

或许更简捷而直接的方法是利用以下事实：任一正整数是 2 的各次幂之和(见第 9 章). 由于 32 本身是 2 的乘幂，所以我们可

按如下方式进行(为了计算方便,可查阅平方数表,例如著名的"巴罗表"):

$$2\equiv 2$$
$$2^2\equiv 4$$
$$2^4\equiv 16$$
$$2^8\equiv 256 \qquad (\text{模均为 } 641)$$
$$2^{16}\equiv 256^2\equiv 65536\equiv 154$$
$$2^{32}\equiv 154^2\equiv 23716\equiv 640\equiv -1$$

*　　*　　*

现在来看魔数 715,364,924. 设 x 是选定的未知数;a,b,c 为它除以 7,11 与 13 的余数,于是有

$$x\equiv a \bmod 7, \qquad 715x\equiv 715a \bmod 7,$$
$$x\equiv b \bmod 11, \qquad 364x\equiv 364b \bmod 11,$$
$$x\equiv c \bmod 13, \qquad 924x\equiv 924c \bmod 13.$$

移项,得

$$715(x-a)\equiv 0 \bmod 7, \tag{1}$$
$$364(x-b)\equiv 0 \bmod 11, \tag{2}$$
$$924(x-c)\equiv 0 \bmod 13. \tag{3}$$

但是(1)式可被 11 与 13 整除,从而也能被 11,13 与 7,即 1001 整除;(2)式可被 7 与 13 整除,亦即能被 7,13 与 11,也就是 1001 整除;(3)式可被7与11整除,从而能被7,11,13,即 [34] 1001 整除. 相加之后,对新模 1001 而言,有:

$$2003x-(715a+364b+924c)\equiv 0 \bmod 1001,$$

或

$$x\equiv 715a+364b+924c \bmod 1001.$$

我们从而获得由三个魔数与三个余数 a,b,c 表达的 x 值,由于它不能超过 1000,于是我们从同余式的右边减去 1001 的整数

倍,以获得限度以下的解答.

作此戏法也可通过一种略有差异的方法.为此,需要记住5,4,-1以及数 $143=11\cdot 13$;$91=7\cdot 13$;$77=7\cdot 11$.对于给定的余数 a,b,c,需求出下面各式的最小剩余:$5a \bmod 7$;$4b \bmod 11$ 以及 $-c \bmod 13$.然后将这些剩余分别乘以143,91与77,把乘积相加,再减去1001的整数倍.例如,若余数为5,6,3,我们有

$$5\cdot 5\equiv 4 \mod 7,$$
$$4\cdot 6\equiv 2 \mod 11,$$
$$(-1)\cdot 3\equiv -3 \mod 13.$$

用143,91,77分别乘上对应的剩余4,2,-3,并予相加,得出 $572+182-231=523$.一些人宁愿使用这种办法,因为涉及的数字较小.记住两套数目5,4,-1与143,91,77也比记住较大的数715,364,924来得容易些.现在,读者们兴许要测试一下自己掌握同余方法的能力,实际推导出这些魔数而不是视为当然.† ①

如果一个同余式对好几个模都成立,则它对这些模的最小公倍数也成立.即若

$$x\equiv a \mod 2,$$
$$x\equiv a \mod 6,$$
$$x\equiv a \mod 8,$$

则

[35] $$x\equiv a \mod 24.$$

利用这一性质,类似下面的问题将很容易解决:有一支部队的人数不能被2,3,4,5,6,7,8,9,10,11,12除尽,在每种情况下

① 带有† 记号的问题在第26章中有解.——原注.

都有一人剩下来.但是,却可以等分为13队.试问,这支部队至少有几人?

这里我们有着关系式:

$$x \equiv 1 \mod 2,3,4,5,6,7,8,9,10,11,12$$

以及

$$x \equiv 0 \mod 13.$$

由于2,3,4,5,6,7,8,9,10,11,12的最小公倍数是27720,从而

$$x \equiv 1 \mod 27720,$$

因此,x需满足的第一个条件是x可等于1或1加上27720的整数倍,亦即

$$x = 27720m + 1.$$

但$27720 \equiv 4 \mod 13$.于是$27720m+1 \equiv 4m+1 \mod 13$,若选取$m=3$,则可得所需的$4m+1 \equiv 0 \mod 13$.因而,满足条件的最小数为$27720 \cdot 3+1=83161$.但$m$可为形如$13n+3$的任意正整数,从而$x$可具有形式$27720(13n+3)+1=360360n+83161$.在$n=0$时,我们即可得到上文所说的83161;当$n=1$时,我们得到第二个解答$x=443521$;其他依此类推.容易验证,用2[①]至12去除这类数时余数都是1,而13恰能整除.

* * *

一个类似的问题如下:有一堆砖头,等分成2堆时剩下1块;分成3堆时剩下2块;分成4堆时剩下3块;……如此类推,但却能正好分成13堆.试问:这堆砖头至少要有多少块?

如果我们一开始就写成:

$$x \equiv 1 \mod 2,$$

① 原文误作1至12,已改正如上.——译者注.

$$x \equiv 2 \mod 3,$$

[36] $$x \equiv 3 \mod 4, \text{等等},$$

则它看上去比上面的问题难解得多. 但我们何必如此不开窍?可以改写为:

$$x \equiv -1 \mod 2,$$
$$x \equiv -1 \mod 3,$$
$$x \equiv -1 \mod 4, \text{等等}.$$

从而

$$x \equiv -1 \mod 27720.$$

于是

$$x = 27720m - 1.$$

故有

$$27720m - 1 \equiv 4m - 1 \equiv 0 \mod 13.$$

但在此情况下,通过试探可知 $m \equiv 10$,这时 39 恰能被 13 整除,于是 $m = 13n + 10$,而

$$x = 27720(13n + 10) - 1 = 360360n + 277199.$$

当 $n = 0$ 时砖数最少,于是 $x = 277199$. 下一个可能值是 $n = 1$,此时砖数为 637559 块.

[37] * * *

许多读者也许听到过荒岛上五名光棍与一只猴子的著名问题. 一天傍晚,流浪汉们收集了一堆椰子,打算在下一天瓜分. 晚间,一个人悄悄起来,把椰子分作相等的五份,把剩下的一只椰子丢给了猴子. 由于对同伴们缺乏信任,他把自己的一份藏在山洞里,重新睡了下去. 余下的四人也都心存猜疑,像上面所说的那位一样进行了类似的操作,每次都私藏起当时全堆的五分之一,并把多余的一只椰子丢给猴子吃了. 下一天,他们把剩下的椰子正好分成五份,但此时却不再有剩下的一只椰子了. 试问:

原先的椰子,至少要有多少只?

本问题可用标准的代数方法去求解,这是就此特例而言.然而,在一般情况,若有"n"人,"r"只猴子,则求解起来就并不如此简单.然而,借助于同余式仍能求解.本书第25章中将给出其解法.

* * *

任一对互质数都具有显著特点:总能找到它们的一些整数倍,使其差数等于1.换言之,对正整数N来说,必存在着N的某个整数倍,使它用另一个与N互质的数去除时其剩余为1,而此时N所乘的倍数恒小于乘积的因子.例如,对15与28而言,必定存在着两个正整数x与y,使得$15x-28y=1$.如果采用同余式记法,则有

$$15x \equiv 1 \mod 28,$$

或

$$28y \equiv -1 \mod 15.$$

存在着直接方法以求解这类同余式,或者解不定方程$ax+by=c$,这里a,b,c是给定的数.一般来说,往往存在着一组以上的解答.下面是一些待解的方程:

1. $71x+37y=3000$.†

2. $599x+107y=100000$.

3. 求出最小正整数b,使方程$1001x+770y=1000000+b$有解,并证明它有100个解.

此类方程的解法,请参看本书第22章.

高阶同余式是数论领域中富有魅力的分支,特别是二次同余式能导出一些极其优美的定理.我们将在讲二次剩余的一章里花费较多时间.

参考文献

Ball, W. W. R. *Mathematical Recreations and Essays*. New York: Macmillan Co., 1939.

Dickson, L. E. *Introduction to the Theory of Numbers*. New York: Dover Publications, Inc., 1957.

Reid, L. W. *Elements of the Theory of Algebraic Numbers*. Baltimore: Johns Hopkins Press, 1946.

Uspensky, J. V., and Heaslet, M. A. *Elementary Number Theory*. New York: McGraw-Hill Book Co., 1939.

Vinogradov, I. M. *Elements of Number Theory*. New York: Dover Publications, Inc., 1954.

[38]

第6章 开 门 咒

算术中有一些定理被认为是“重要的”，而其他一些定理尽管同样难以证明，却被说成微不足道．要说明何以如此，即便不是不可能，也是很困难的．一个标准（虽然不一定是结论性的）是这个定理应该能运用到数学的其他领域中去；另一个标准是，它应该启发算术或广义的数学中的研究；第三个是，它在某些方面应该是带有普遍性的．刚才叙述的费马定理满足所有这些多少有些武断的要求……它在下述意义上带有普遍性：它描述了所有素数的一个性质——要找出如此一般化的论述是极其困难的，已经知道的东西实在是少而又少．

——E·T·贝尔《数学精英》

在日常事务中我们经常运用一种称为归纳推理的逻辑过程．从观察到的一系列事实进行推广，试图得出某种规律．许多个春天花朵盛开，于是可以放心地推论：只要春天来临，花儿都会盛开．然而，在数学里头，归纳推理好得不够．你会发现，在某些条件下有的事实一次成立，二次成立，甚至一百次也成立．如果你不经心地说，“它永远是对的”，那么有可能在下一次，你的断言就不对了．数学所需要的远远不止是仅依靠观察得来的归纳推理．而所谓数学归纳法却是能满足这种需求的方

法.

数论中充斥着易于观察到的事实,诱使人们用普通归纳推理去进行推广. 对此,人们必须慎之又慎,以免误入陷阱. 设想你把 2 自乘 7 次,再减去 2,即 $2^7-2=126$,它恰能被指数 7 整除. 另外,2^5-2 能被 5 整除;$2^{11}-2$ 能被 11 整除. 接着,你又去试验 2^4-2,它不能被 4 整除;还有,2^6-2 不能被 6 整除;2^8-2 不能被 8 整除.

或许你会停顿一下,进行总结:指数为奇数时,表达式似能整除;指数为偶数时,则不能整除. 为了确证,手边又有点空余时间,你便测试一下 $2^9-2=510$ 并惊讶地发现它是不能被 9 除尽的,还有 $2^{15}-2=32766$ 也不能被 15 除尽. 显然需要修正你匆忙作出的结论. 此时,一个想法开始露头;对 2,3,5,7,11 规则成立而对 4,6,8,9,10,12,14,15 却不成立. 证据似乎变得明显.

[39]

当指数为素数时出现了整除性;当指数为合数时则不然. 你关于奇数和偶数的初步设想显然是站不住脚了. 如果你感到非常惊讶,那就不妨从 16 一直试到 25,在这段范围内含有合数 21,25 以及 17,19,23 等素数. 显然 $2^{17}-2$,$2^{19}-2$,$2^{23}-2$ 能相继被 17,19 与 23 整除,然而所有的偶指数组合以及 $2^{21}-2$,$2^{25}-2$ 均不能被其指数除尽.

不过,你的结论仍旧需要作出校正. 早在公元前 500 年,中国人就已经认为:当 p 是素数时,2^p-2 必能为 p 整除,而当 p 为合数时,2^p-2 一定不能被 p 整除. 实际情况又怎样呢? p 为素数时,2^p-2 恒能为 p 整除固然不错,可是 p 为合数时 2^p-2 不能为 p 整除却是不对的. 最小的合数指数却能使整除成立的是 $341=31\cdot 11$,而 $2^{341}-2$ 却恰巧能被 341 整除. 这一事实晚到 1819 年才被发现. 如用通常办法,你将用掉好几个小时才能证明这一点,但如果用同余式,寥寥数步即可办到.

号称"业余数学王子"的皮埃尔·德·费马重新发现了这一

早在孔夫子时代即已为人忘却的规律并将原结果推广：若 p 为素数，则 x^p-x 必能被 p 整除. 他是作出了证明的，此事虽然简单但很难捉摸，费马办成了以前中国人做不到的事. 就一般结果而言，x 当然可以是任何正整数，而不一定仅限于 2. 如果我们把 x^p-x 提取因子，即 $x(x^{p-1}-1)$，则根据定理，此式应能被 p 整除. 现设 x 不是 p 的倍数，即 p 不能整除 x，则若 p 能整除整个表达式的话，p 必然能整除 $x^{p-1}-1$. 于是，我们由此获得费马小定理的常见形式：

"若 x 是一个不能为素数 p 整除的整数，则 $x^{p-1}-1$ 必能被 p 整除."若用同余式写法(见第 5 章)，便是 $x^{p-1}\equiv 1 \bmod p$.

这种朴实无华的代数关系似乎不会给人们留下什么深刻印象. 然而它导致了众多的思维与奥妙的数学逻辑通道，因而被看 [40] 成是数论大厦的一块基石. 对如此美妙的定理而居然毫不动心者肯定是只剩一口气的行尸走肉吧！类似

$$2^{134217826}-1$$

这样的一个大数，它有着四千万位数字，需要 40 卷 500 页的大书(每页 2000 字)才能容纳得下. 然而根据费马定理，我们立即可以肯定它能被数 134217827 整除无余.（当然我们应被告知 134217827 确是一个素数.）

本定理有多种证法；同余证法既简短又精致. 在证明时，让我们任意选取素数 13，当然如果我们选用其他任意素数 p，证法也几乎同样简单. 现在考虑从 1 到 12 的一系列整数 1,2,3,…,12，每一个都比 13 小. 若我们对这些数的每一个都乘上一个与 13 互质的整数，譬如 3，我们即可得出 3,6,9,12,15,18,…,36. 对模 13 而言，这些数同余于 3,6,9,12,2,5,8,11,1,4,7,10. 其中并无重复，实际上它们就是原来的 1,2,3,4,…,12，只不过是顺序不同而已.

现在让我们把原先一系列数统统相乘起来，其乘积便是 1·2

$\cdot 3 \cdot \cdots \cdot 12$，也可方便地记作 12!，并读作"12 的阶乘"（这可从代数学中回忆起来）．如果类似地把 3，6，9，…，36 相乘，可以先提出公因子 3，并把乘积记作 $3^{12} \cdot 12!$．对模 13 而言，这两个乘积互相同余，因为 3，6，9，…，36 的系列同余于 1，2，3，…，12 的系列，尽管不是前后都一一对应．因而 $3^{12} \cdot 12! \equiv 12! \bmod 13$，除以 12!之后，便得出 $3^{12} \equiv 1 \bmod 13$．如果我们用 p 代替 13，用 x 代替 3，则我们即能得到 $x^{p-1} \equiv 1 \bmod p$，也就是费马小定理．（为了简单起见，此处已经省略了若干使证明"严格"的细节．）

如果费马定理只是对素数成立，人们就能得到判定素数的一个实用准则．因若某数 p 能整除 $x^{p-1}-1$，则除数必为素数；否则它就是合数．不幸的是，我们并没有此种实用准则．费马定理对素数永远成立，对合数则有时也成立．在这方面，定理之逆经常被人误解了．

令人惊讶的是，居然可以找到无穷多个合数使关系式成立．[41] 除了上面的例子以外，我们还有 $3^{90}-1$ 可以被 91 整除；$4^{14}-1$ 可以被 15 整除，如此等等．对 2 至 100 的一切底数，这类大于底数的最小合数除数见附表 15．

请注意，最小底数 2 竟然需要一个很大的除数 341，从此起底数一直上到 100，没有哪个除数超过 341．因此无人会怀疑，中国人未能找到他们用归纳法发现的规律之例外．在第 13 章中将要说明，这类合数除数是怎样发现的．

合数除数有两个有趣问题：

1. 底数 x 为某些已知数时，使费马定理成立的这类除数的决定．

2. 对任何与合数除数互质的底数 x，使费马定理成立的这类除数的决定．

就第一个问题而言，表 15 为直至 100 为止的每个底数提供了一个解答．对任意特定底数，当然会有许多解．我们在附表 16 与 17 中，已经对底数 2 与 3 提供了一些例子．

底$=x$	除数$=m$	底$=x$	除数$=m$	底$=x$	除数$=m$
2	$341=11\cdot31$	35	$51=3\cdot17$	68	$69=3\cdot23$
3	$91=7\cdot13$	36	$91=7\cdot13$	69	$85=5\cdot17$
4	$15=3\cdot5$	37	$45=3^2\cdot5$	70	$169=13^2$
5	$124=2^2\cdot31$	38	$39=3\cdot13$	71	$105=3\cdot5\cdot7$
6	$35=5\cdot7$	39	$95=5\cdot19$	72	$85=5\cdot17$
7	$25=5^2$	40	$91=7\cdot13$	73	$111=3\cdot37$
8	$9=3^2$	41	$105=3\cdot5\cdot7$	74	$75=3\cdot5^2$
9	$28=2^2\cdot7$	42	$205=5\cdot41$	75	$91=7\cdot13$
10	$33=3\cdot11$	43	$77=7\cdot11$	76	$77=7\cdot11$
11	$15=3\cdot5$	44	$45=3^2\cdot5$	77	$95=5\cdot19$
12	$65=5\cdot13$	45	$76=2^2\cdot19$	78	$341=11\cdot31$
13	$21=3\cdot7$	46	$133=7\cdot19$	79	$91=7\cdot13$
14	$15=3\cdot5$	47	$65=5\cdot13$	80	$81=3^4$
15	$341=11\cdot31$	48	$49=7^2$	81	$85=5\cdot17$
16	$51=3\cdot17$	49	$66=2\cdot3\cdot11$	82	$91=7\cdot13$
17	$45=3^2\cdot5$	50	$51=3\cdot17$	83	$105=3\cdot5\cdot7$
18	$25=5^2$	51	$65=5\cdot13$	84	$85=5\cdot17$
19	$45=3^2\cdot5$	52	$85=5\cdot17$	85	$129=3\cdot43$
20	$21=3\cdot7$	53	$65=5\cdot13$	86	$87=3\cdot29$
21	$55=5\cdot11$	54	$55=5\cdot11$	87	$91=7\cdot13$
22	$69=3\cdot23$	55	$63=3^2\cdot7$	88	$91=7\cdot13$
23	$33=3\cdot11$	56	$57=3\cdot19$	89	$99=3^2\cdot11$
24	$25=5^2$	57	$65=5\cdot13$	90	$91=7\cdot13$
25	$28=2^2\cdot7$	58	$95=5\cdot19$	91	$115=5\cdot23$
26	$27=3^3$	59	$87=3\cdot29$	92	$93=3\cdot31$
27	$65=5\cdot13$	60	$341=11\cdot31$	93	$301=7\cdot43$
28	$87=3\cdot29$	61	$91=7\cdot13$	94	$95=5\cdot19$
29	$35=5\cdot7$	62	$63=3^2\cdot7$	95	$141=3\cdot47$
30	$49=7^2$	63	$341=11\cdot31$	96	$133=7\cdot19$
31	$49=7^2$	64	$65=5\cdot13$	97	$105=3\cdot5\cdot7$
32	$33=3\cdot11$	65	$133=7\cdot19$	98	$99=3^2\cdot11$
33	$85=5\cdot17$	66	$91=7\cdot13$	99	$145=5\cdot29$
34	$35=5\cdot7$	67	$85=5\cdot17$	100	$259=7\cdot37$

表 15　大于底数 x 的最小合数除数 m，可使 $x^{m-1}-1$ 得以被 m 整除　[42]

$m=$
11 • 31
23 • 89
3 • 5 • 43
3 • 5 • 29 • 43
3 • 5 • 29 • 43 • 113
3 • 11 • 29 • 31 • 43 • 281
7 • 11 • 13 • 31 • 41 • 61 • 331
7 • 11 • 13 • 31 • 41 • 61 • 151 • 1321
3 • 11 • 29 • 31 • 41 • 43 • 71 • 113 • 127 • 281
5 • 7 • 17 • 19 • 37 • 73 • 97 • 109 • 241 • 433 • 673 • 38737

表 16　使 $2^{m-1}-1$ 能被 m 整除的合数除数 m

当 p 是一个素数，而 2^p-1 为合数时，则满足 $m=2^p-1$ 的一切 m 也都行.

$m=$
23 • 3851
17 • 193
19 • 37
31 • 271

表 17　能使 $3^{m-1}-1$ 被 m 整除的合数除数 m

[43]

*　　*　　*

第二个问题更困难些. 譬如说，$2^{340}-1$ 能被 341 整除，可是 $3^{340}-1$ 却不行. 读者们不妨再次运用新获得的同余知识来验证一下. 与此类似，$3^{90}-1$ 能被 91 整除，可是 $2^{90}-1$ 不然. 这里的问题是要找出合数 n，使对与 x 互质的一切整数，$x^{n-1}-1$ 都能被 n 整除. 问题的解并不太容易. 至少得有三个素数因子组成除数. 最小解为 $x^{560}-1$，它能被合数 $561=3\cdot 11\cdot 17$ 所整除. 此处 x 可取任意值，除了 3，11，17 或其倍数之外. 即是说 $2^{560}-1$ 能被 561 整除，$4^{560}-1$，$5^{560}-1$，$7^{560}-1$ 等等也行. 这真是一个值得注意的关系. 此种合数为数甚少并且相互之间隔得很远.

若合数模 n 正好含有三个素因子，若对其中的一个因子 p

指定一个值,则其他两个素因子只能取有限个值,它们也不能无限递增.从 3 到 43 之间指定 p 值,一共只有 52 个可能的合数模.奇怪的是,$p=11$ 时无解.这 52 个值已列举在附表 18 之中.

3·11·17	19·43·409	41·61·101
5·13·17	19·199·271	41·73·137
5·17·29	23·199·353	41·101·461
5·29·73	29·113·1093	41·241·521
7·13·19	29·197·953	41·241·761
7·13·31	31·61·211	41·881·12041
7·19·67	31·61·271	41·1721·35281
7·23·41	31·61·631	43·127·211
7·31·73	31·151·1171	43·127·1093
7·73·103	31·181·331	43·127·2731
11 无解	31·271·601	43·211·337
13·37·61	31·991·15361	43·211·757
13·37·97	37·73·109	43·271·5827
13·37·241	37·73·181	43·433·643
13·61·397	37·73·541	43·547·673
13·97·421	37·109·2017	43·631·1597
17·41·233	37·613·1621	43·631·13567
17·353·1201		43·3361·3907

表 18 对一切与模互质的底数,$a^{n-1}\equiv 1 \bmod n$ 都成立的合数模 n [44]

在这个问题上登峰造极的、由四个素数构成的合数 n 是

$$n = 13 \cdot 37 \cdot 73 \cdot 457 = 16046641,$$

它使 $a^{16046640}\equiv 1 \bmod 16046641$ 成立.

* * *

在逻辑学里,有一种关系名为"蕴含":"若p则q,"其逆命题是"若q则p."逆命题可以有时为真,但不一定永远是真.除了逆命题,还有反命题,"若非 p,则非 q."这种反命题,同样也仅有时为真.但还有逆反命题,"如非 q,则非 p,"这是永远为真的命题.把这些知识应用到费马小定理,设 p 是"一素数",q 是"$x^{p-1}\equiv 1 \bmod p$."则逆命题"若 $x^{p-1}\equiv 1 \bmod p$,则 p 是一个素数",仅能有时为真,因为对某些合数来说,也存在着此种关系式,附表

18已表明了这一点.反命题"若p不是素数,则$x^{p-1}\not\equiv 1 \bmod p$"也并非永远是真,正如表18所示.然而逆反命题"如果x^{p-1}对模p不与1同余,则p不是素数(是合数)"必定永远为真.

费马小定理的真正"逆说法"是:若一正整数x与m互质并且$x^{m-1}\equiv 1 \bmod m$,而不存在一个小于$m-1$的正整数e,能使$x^e\equiv 1 \bmod m$成立,则m是一素数.例如$3^{16}\equiv 1 \bmod 17$,但小于16的任何指数都不能使同余式成立,所以17是一个素数.这当然并不意味着,如果确实找得出一个e的话,m就不是素数了.譬如说,$2^6\equiv 1 \bmod 7$与$2^3\equiv 1 \bmod 7$都是成立的,然而7仍是素数.不过,若把3选作为底的话,6兴许便是最小的指数了.

到此地步,可以引入两个今后用得上的新名词.如果$x^e\equiv 1 \bmod m$而e是使同余式成立的最小指数,则我们称为"x属于指数e,模m."另一方面,若此最小指数是$m-1$,则我们就说"x是m的一个原根."原根是有更一般化的定义的,但此种说法在目前可为我们服务.在$2^3\equiv 1 \bmod 7$中,2属于指数3,模7;在$3^6\equiv 1 \bmod 7$中,3是7的一个原根.

费马小定理只是更一般的,同时可适用于素数与合数模的一个定理的推论.该定理的说法是:若x与m无公因子,而m是任一正整数(素数或合数),则$x^{\phi(m)}-1$必能被m整除.这里,表达式$\phi(m)$当然并不意味着ϕ去乘m.它是指小于m且与之互质的正整数的个数.设m是一个素数,则每一个小于它的正整数都同它互质,于是$\phi(m)=m-1$.这就导出费马小定理.作为一般情形的特例,可以看一下数15.小于15且与之互质的数的个数为8,那就是1,2,4,7,8,11,13,14.(数1视为与任何其他正整数互质.)于是$\phi(15)=8$,若x为任一与15互质的数,则x^8-1能被15整除.例如$2^8-1=255$能行,$7^8-1=5764800$也能行,如此等等.

[45]

*　　*　　*

有时候,$x^{p-1}-1$可被p整除多次.例如$3^{10}-1$可被$11^2=$

121 整除，$9^{10}-1$ 亦然. 许多研究者曾经以为对底数 2 与 10 来说，此类解答是不可能的. 只是到了最近，才发现 $2^{1092}-1$ 能被 1093^2 整除；而 $2^{3510}-1$ 能被 3511^2 整除，$10^{486}-1$ 能被 487^2 整除. 更奥妙的是 $68^{112}-1$，它竟能被 113^3 整除. 除去 1093 与 3511 外，对底数 2 而言，再也找不出在 200183 以下的素数能使关系式成立. 事实上，已经找到一些底数，使关系式对任意指定素数的平方也能成立. 表 19 中，列出了一些数据，可使 $x^{p-1}-1$ 能被 p^2 整除.

x	p	x	p	x	p	x	p
2	1093	18	37	31	79	62	127
2	3511	18	331	38	17	65	163
3	11	19	7	38	127	68	113
7	5	19	13	43	103	69	631
8	3	19	43	51	41	71	331
9	11	19	137	53	3	78	151
10	487	22	673	53	47	78	181
11	71	26	71	53	59	84	163
14	29	28	19	53	97	96	109
18	7	28	23	58	131	99	83

表 19　$x^{p-1}\equiv 1 \bmod p^2$

前已说过，对任意素数的平方，此类解答都能找到，作为其实际例证，我们在表 20 中给出了在表 19 中没有提到过的小于 200 的一切素数.

[46]

p	x	p	x	p	x
31	115	101	181	173	259
53	338	107	164	179	532
61	264	139	328	191	176
67	143	149	313	193	276
73	306	157	226	197	143
89	184	167	253	199	174

表 20　$x^{p-1}\equiv 1 \bmod p^2$

表 21 给出了一些很大的数值，其中也包括素数的若干高次

方，而不光是平方.

a	x	p	a	x	p	a	x	p
2	100	487	3	18	7	4	239	13
2	175	487	3	19	7	5	1353	7
2	196	353	3	158	17	5	1354	7
2	252	997	3	338	19	6	1068	5
2	307	487	4	2819	19	6	390112	17
2	324	331	4	2820	19	7	82681	7
2	484	673				7	82682	7

表 21　$x^{p-1}\equiv 1 \bmod p^a$

*　　　*　　　*

所谓“费马商”$(2^{p-1}-1)/p$ 仅对两个素数值给出完全平方数. 读者能否把它们找出来？† ①

人们经常感到费马定理有朝一日会变成打开无价数学宝藏的“开门咒”，这些宝贝目前埋藏得很深，现世的肉眼凡夫还未能认识得到. 人们甚至猜想，那位神秘的鬼魂正在暗暗嘲笑 20 世纪的现代凡夫，他们尽管在其逝世之后作出了许多深奥难懂的发现，却仍在徒劳无功地追踪着迷失的大师足迹.

参考文献

Barlow, P. *Theory of Numbers*. London: J. Johnson & Co., 1811.

Beeger, N. G. W. H. “Quelques Remarques sur les Congruences $r^{p-1}\equiv 1 \pmod{p^2}$ et $(p-1)!\equiv -1 \pmod{p^2}$,” *Messenger of Mathematics*, **43**(1913), 73. [47]

——. “On Composite Numbers, n, for Which $a^{n-1}\equiv 1 \bmod n$ for Every a Prime to n,” *Scripta Mathematica*, **16**(1950), 133.

① 用†标出的问题在第 26 章中有解答. ——原注.

Bell, E. T. *Men of Mathematics*. New York: Simon and Schuster, 1937.

Bickmore, C. E. "On the Numerical Factors of a^n-1," *Messenger of Mathematics*, **25**(1895), 1.

Carmichael, R. D. *Theory of Numbers and Diophantine Analysis*. New York: Dover Publications, Inc., 1959.

——. "On Composite Numbers P Which Satisfy the Fermat Congruence $a^{P-1} \equiv 1 \bmod P$," *American Mathematical Monthly*, **19**(1912), 22.

Cunningham, A. *Haupt-Exponents, Residue Indices, Primitive Roots*. London: F. Hodgson, 1922.

——. "Problem: Find Numbers N, Such that $1/N^2$, etc., Have the Same Number of Figures in the Scale of Radix r," *Mathematical Gazette*, **4**(1907—1908), 209.

——. "Period Lengths of Circulates," *Messenger of Mathematics*, **29**(1898—1899), 145.

——. "Haupt-Exponents of 2," *Quarterly Journal of Pure and Applied Mathematics*, **37**(1905), 122.

——. "On Haupt-Exponents of 2," *Quarterly Journal of Pure and Applied Mathematics*, **42**(1911), 241.

——. "On Haupt-Exponents of 2," *Quarterly Journal of Pure and Applied Mathematics*, **44**(1912—1913), 41.

——. "On Haupt-Exponents of 2," *Quarterly Journal of Pure and Applied Mathematics*, **44**(1912—1913), 237.

——. "On Haupt-Exponents of 2," *Quarterly Journal of Pure and Applied Mathematics*, **45**(1914), 114.

Dickson, L. E. *History of the Theory of Numbers*. 3 vols. New York: Chelsea Publishing Co., 1950.

——. *Introduction to the Theory of Numbers*. New York:

Dover Publications, Inc., 1957.

Escott, E. B. "The Converse of Fermat's Theorem," *Messenger of Mathematics*, **36**(1906), 175.

Herzer, H. "Über die Zahlen der Form $a^{p-1}-1$, wenn p eine Primzahl," *Archiv der Mathematik und Physik*, **13**—**14**, Series 3(1908—1909), 107.

Kraitchik, A. M. *Recherches sur la Théorie des Nombres*. Paris: Gauthier-Villars et Cie., 1924.

Lehmer, D. H. "On the Converse of Fermat's Theorem," *American Mathematical Monthly*, **43**(1936), 347.

Pearson, E. H. "On the Congruences $(p-1)! \equiv -1$ and $2^{p-1} \equiv 1 \bmod p^2$," *Mathematics of Computation*, **17**(1963), 194.

Reid, L. W. *Elements of the Theory of Algebraic Numbers*. Baltimore: Johns Hopkins Press, 1946.

Rosser, B. "On the First Case of Fermat's Last Theorem," *Bulletin of the American Mathematical Society*, **45**(1939), 636.

Vandiver, H. S. "Divisibility Problems in Number Theory," *Scripta Mathematica*, **21**(1955), 16.

Vinogradov, I. M. *Elements of Number Theory*. New York: [48] Dover Publications, Inc., 1954.

第7章 难解饥渴[①]

一位不显眼的英国法官在数学忠烈祠中居然被供奉着，因为据说是他发现了数论中极为稀罕的关系，而且逆定理也成立．他对此事并不介意，如果不是他的朋友爱德华·华林(Edward Waring)，剑桥大学的数学教授发表了他的研究成果的话，那就十之八九会像费马小定理一样，遭到彻底遗忘，或者在多年之后再重新发现的．

但是，约翰·威尔逊爵士(Sir John Wilson)也好，他的好朋友华林也好，甚至微积分的共同发明家，先于威尔逊发现这一数论定理的莱布尼茨(Leibnitz)都没有能够证明该定理的正确性．早在17世纪结束前许多年，莱布尼茨即已知道该定理了；1770年，华林在他的代数学著作中报告了威尔逊的发现；拉格朗日(Lagrange)在1771年证明了它，在莱布尼茨首先发表之后一百多年．因此，为了公正起见，应当把它命名为莱布尼茨定理，而不是"威尔逊"定理．但是，正如经常发生的事实一样，某项重大成就一旦归功于某人名下之后，即便是罗马教皇的圣旨也改变不了它．

下文便是威尔逊重新发现的事实：取所有连续正整数的乘

---

① 本章原标题直译为"坦塔罗斯之杯"．据希腊神话，坦塔罗斯为天神宙斯之子，因泄漏天机被罚，永世站立在上有果树的水中．口渴想喝水时水却减退；腹饥想吃果子时，树枝即升高．——译者注．

积，从1取到某个素数，例如11，并写下其乘积：1·2·3·4·5·6·7·8·9·10·11. 换一下记号，它可以浓缩为11!，读作"11的阶乘". 容易看出11!能被1到11(包括11)的一切整数整除. 现在略去11，把余下十个正整数乘起来，显然10! 是不能被11整除的，因为11是个素数，而不含11或其倍数的乘积当然不能被11除尽. 然而如果我们在积10! 之上再加1的话——就像变戏法，说变就变！所得的结果恰能被11整除. 类似地 6!+1=(1·2·3·4·5·6)+1=721能被7整除. 7与11都是素数，此种整除性对一切素数都成立，但对合数却永不成立.

把上面所说的加以推广，当且仅当 p 为素数时，$(p-1)!+1$ 能被 p 整除. 这就是威尔逊定理，它的若干推论与推广是极重要的——实际上费马小定理即可由其中的一个推广导出.[49]

表22说明威尔逊定理怎样用于测试素数.

n	$(n-1)!$		$(n-1)!+1$	$[(n-1)!+1]\div n$ 的余数	性质
2	1! =	1	2	0	素数
3	2! =	2	3	0	素数
4	3! =	6	7	3	合数
5	4! =	24	25	0	素数
6	5! =	120	121	1	合数
7	6! =	720	721	0	素数
8	7! =	5040	5041	1	合数
9	8! =	40320	40321	1	合数
10	9! =	362880	362881	1	合数
11	10! =	3628800	3628801	0	素数
12	11! =	39916800	39916801	1	合数
13	12! =	479001600	479001601	0	素数
14	13! =	6227020800	6227020801	1	合数
15	14! =	87178291200	87178291201	1	合数

表22 判定素数的威尔逊准则

从理论上看，要判别一个数是否素数，本定理是个判别准则. 例如，要问421783是不是素数，只要把1到421782的所有正整数统统乘起来，再加上1，看一看所得之结果能否被421783

整除.除得尽,它是素数;除不尽,它便是合数.尽管如此,对这么一个较小的六位数,工作量已经大得惊人,根本无法使用此种判别法.用同余式或其他手段来计算$(n-1)!+1$除以n的余数也非常困难.因此,尽管我们手头已经有了足以判定素数的结论性测试法,基于实际可操作性,我们还是窥探不到数的本性.

本定理有许多美妙证法.为了避免过分技术化,让我们采取第6章中证明费马小定理的同样办法,通过一个特定素数来加以证明.我们打算起用素数$p=17$.考虑小于17的十六个正整数1,2,3,…,16,再次选用小于17的数3来作出乘积3,6,19,12,…,48.对模17而言,这些数目相应地与下面一些数目3,6,9,12,15,1,4,7,10,13,16,2,5,8,11,14同余.这里头没有重复数字(一般情况下亦易证明).因而其中必有一数为1,对本例来说,即第六数.如果用另一个乘数来代替数3,例如改用5,则可得到另一列数,其中肯定有个1,譬如说$5\times7\equiv1 \bmod 17$.在一系列数2,3,4,…,15中的每一个都可用作乘数,结果出现七对数,而每对数的乘积按模17同余于1,即: [50]

$$\left.\begin{aligned}2\cdot9&\equiv1\\3\cdot6&\equiv1\\4\cdot13&\equiv1\\5\cdot7&\equiv1\\8\cdot15&\equiv1\\10\cdot12&\equiv1\\11\cdot14&\equiv1\end{aligned}\right\}\bmod 17.$$

故在系列1,2,3,…,16中,除了首、尾二数之外,统统都已结成对子,而对首、尾二数,则有

$$1\cdot16\equiv-1 \bmod 17.$$

这个例子正可用来证明我们的定理.

把这八个同余式相乘,于是得出

$$16! \equiv -1 \bmod 17.$$

也就是说，$(17-1)!+1$ 能被 17 整除，这就是我们所要证明的. 只需略作改变，即可证明一般情形. 即，若 p 为素数，则

$$(p-1)!+1 \equiv 0 \bmod p.$$

集合中的各数竟能以如此方式结成对子，且无重复、遗漏，真正奇妙之至！

同费马定理一样，威尔逊定理也有若干推广. 例如并不一定要把模限于素数，只需修改我们的法则：小于某个定数且与之互质的一切正整数的乘积在用该定数去除时余数为 1，但下列情况例外：若定数是 4，或者一个素数的方幂，或者该方幂的二倍，此时余数将是 -1. 设给定数是 12，它既非一素数之方幂，亦非其二倍. 这时，与 12 互质的一切正整数之积为 $1\cdot5\cdot7\cdot11=385$，它在除以 12 时留下余数 1. 若定数为 4，则有 $1\cdot3$，它留下余数 -1. 对一个素数方幂例如 $3^2=9$ 而言，则有 $1\cdot2\cdot4\cdot5\cdot7\cdot8=2240$，在除以 9 时留下的余数为 -1. 最后，我们不妨用素数方幂的二倍来试一试，譬如说 $18=2\cdot3^2$，此时将得出 $1\cdot5\cdot7\cdot11\cdot13\cdot17=85085$，它按模 18 同余于 -1.[51]

*　　*　　*

在很稀少的场合，$(p-1)!+1$ 不仅能被 p 整除，甚至能被 p^2 整除. 对小于 200183 的素数而言，此事仅在 5，13 以及 563 时才对. 其时将有

$$(5-1)!+1=25=5^2\cdot1;$$
$$(13-1)!+1=479001601=13^2\cdot2834329;$$
$$(563-1)!+1=563^2\cdot N.$$

N 是一个极其庞大的数.

*　　*　　*

威尔逊定理有一个推论走得很远. 它说当且仅当素数 p 具

有 $4x+1$ 形状时，

$$(1\cdot 2\cdot 3\cdot \cdots \cdot 2x)^2+1$$

是 p 的一个倍数，也就是说，$[(2x)!]^2\equiv -1 \mod p$. 例如，$x=3$ 时，素数 13 恰能整除

$$(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6)^2+1=518401.$$

证明很简单，可在此处给出. 我们从 $4x$ 开始，它显然与 -1 同余，$\mathrm{mod}(4x+1)=p$；例如，数 12 在被 13 去除时，余数是 -1. 于是我们有：

$$4x\equiv -1 \mod p,$$
$$4x-1\equiv -2 \mod p,$$
$$4x-2\equiv -3 \mod p.$$

就这样，从 $4x$ 起每回递减 1，来写 $2x$ 个同余式，直到 $4x-(2x-1)=2x+1$，于是有

$$2x+1\equiv -2x \mod p.$$

把这些同余式乘在一起，但此时的代数表达式改作始于 $2x+1$ 逐一递增的连续正整数，而不是从 $4x$ 递减，于是得出

$$\begin{aligned}(2x+1)(2x+2)\cdots 4x &\equiv (-1)^{2x}(1\cdot 2\cdot 3\cdot 4\cdot \cdots \cdot 2x)\\ &\equiv +1(2x)!\end{aligned}$$

在同余式两端同时乘上 $(2x)!$，得出

$$(4x)!\equiv [(2x)!]^2,$$

[52]

由原先的威尔逊定理，$(4x)!+1\equiv 0 \mod p$，代入后，即得 $[(2x)!]^2+1\equiv 0 \mod p$.

本定理是一串美妙逻辑推理中的第一节. 它证明了，形如 $4x+1$ 的素数必可表示为两个整数的平方和，而且表达法是唯一的. 继起的环节表明，由两个互质的平方数之和来表示的合

数，其除数也是两平方数之和. 作为特例，对素数除数亦然. 然而，$[(2x)!]^2+1$ 是两个平方数之和，因此它的每一个除数也必然是两平方数之和. 既然 $4x+1$ 形式的素数 p 可表示为两个平方数之和，所以形为 $4x+1$ 的任一素数 p 可表示为两个平方数之和，当然它们必须是互质的.（如果两个正整数除 1 之外没有其他公因子，就说它们是互质的. "互质"与"互素"是同义词，意思完全一样.）

*　　*　　*

形如 $4x-1$ 的素数 p 不可能是两个平方数之和. 由于 p 是奇数，两个平方数必定一奇一偶. 但是每一偶数平方 $(2A)^2$ 具有形状 $4A^2$，而任一奇数平方 $(2B+1)^2$ 具有形状 $4B^2+4B+1$，于是其和

$$4A^2+4B^2+4B+1$$

必定具有 $4x+1$ 的形状，决不可能取 $4x-1$ 的.

参考文献

Barlow, P. *Theory of Numbers.* London: J. Johnson & Co., 1811.

Carmichael, R. D. *Theory of Numbers and Diophantine Analysis.* New York: Dover Publications, Inc., 1959.

DeMorgan, A. *Budget of Paradoxes.* 2 vols. Chicago: Open Court Publishing Co., 1915.

Dickson, L. E. *Introduction to the Theory of Numbers.* New York: Dover Publications, Inc., 1957.

Pearson, E. H. "On the Congruences $(p-1)!\equiv -1$ and $2^{p-1}\equiv 1 \mod p^2$," *Mathematics of Computation*, **17**(1963), 194.

Reid, L. W. *Elements of the Theory of Algebraic Numbers.* Baltimore: Johns Hopkins Press, 1946.

Uhler, H. S. "Nine Exact Factorials Between 449! and 751!," *Scripta Mathematica*, **21**(1955),138.

Vandiver, H. S. "Divisibility Problems in Number Theory," *Scripta Mathematica*, **21**(1955),16.

Vinogradov, I. M. *Elements of Number Theory*. New York: Dover Publications, Inc., 1954. [53]

第8章　数码与9的魔术

数码9的奇异性质经常被魔术家与术数家①利用，是一些戏法的基础.早在古代，此数即已激起学者与数学家们的兴趣，并且出现了一些连门外汉也能理解与欣赏的数字戏法.读者们可能会回忆得起在初等学校里学到的规则，如果某数的各位数码之和能被9整除，则此数必然也能被9整除.一个引人注目的事例曾于数年前披露于一家通俗杂志上：有一等式 $2A99561=[3(523+A)]^2$，要求你在60秒钟内求出数码 A，看来这显然不可能.然而，一个思路敏捷者会看到，表达式的右边含有 $3^2=9$ 这一因子，所以表达式的左边也应能被9整除.除 A 之外，它的其他各位数码加起来等于32，于是马上就可判定 A 必然为4，只有如此，各位数码之和36才能被9整除.

"弃九法"(有时也叫"印度验算法")经常被簿记员用来检验加法运算是否正确，但它对任何一个算术四则运算都能适用.所依据的基本事实是：一个数的各位数码之和与此数本身在被9除的时候，余数是相同的.数码和的余数为0，亦即该数本身被9除时的余数为0，这意味着此数可以被9整除，也就是以前提到的法则.把这些知识记在心里，下面两个用以说明弃九法的加法

---

① 术数家在我国古代即已有之.近代西方国家的巫师往往利用数学来预测算命.其中一个颇有代表性的人物便是马丁·加德纳笔下的阵图博士(Dr. Matrix).——译者注.

与乘法实例,就可以不言而喻了.

加法	各位数码和被9除的余数
4671	0
2198	2
7422	6
5611	4
1105	7
总和 21007	19=余数之和

[54]

和数的各位数码相加起来等于10,而余数之和的数码之和也是如此,这就是整个验算过程.此种校验尽管不是绝对可靠,但加法中出现的差错不大可能会"碰巧"抵销而得出正确余数的.另一种可取的办法是,当数码和超过10时,可以继续执行上述运算,直至得出一个小于9的结果.例如,对21007而言,数码和是10,而后者的数码和是1.对19也是如此.这就表明,数21007被9除时,余数为1.

乘法		数码和被9除的余数
被乘数	5327	8
乘数	649	1
	47943	
	21308	
	31962	
乘积	3457223	8

这里,积的数码和等于26,而2+6=8,恰恰就是余数8与1相乘积的数码和.

同余方法对这些测试的说明近于自明.例如,对上述加法实例,模为9,我们有:

$$
\begin{aligned}
4671&\equiv 0\\
2198&\equiv 2\\
7422&\equiv 6\\
5611&\equiv 4\\
1105&\equiv 7\\
\hline
21007&\equiv 19\equiv 1
\end{aligned}
$$

*　　　　*　　　　*

"随便你写出一个很大的数，从中抹掉一个数码，我再填入一个，使该大数恰能被 9 整除，"诸如此类的戏法简直易如反掌了.例如：

[55]　　53219645 * 2789，

只要把各位数码相加，其和是 61.6 与 1 之和是 7，显然填入的数码应当是 2.也可以把戏法稍作修改，要求填进一个数码之后，整个大数被 9 去除后，得到的余数等于事先指定的数码.

这种潜伏于数码 9 中的戏法，本质上当然在于我们所用的乃是十进位记数制，而一个数中的某位数码实际上代表该数码与 10 的某个方幂之积.例如，7312 实际是

$$(7\cdot 10^3)+(3\cdot 10^2)+(1\cdot 10^1)+2,$$

而 907450 是

$$(9\cdot 10^5)+(0\cdot 10^4)+(7\cdot 10^3)+(4\cdot 10^2)+(5\cdot 10^1)+0.$$

这种办法称为"位值制"，除去绝对数值外，每位数码的局部值取决于它在整个数字中所处的位置.一旦理解了这一点，余数测试的原理就易于理解了.

对模 9 而言，

$$10\equiv 1,$$

从而

$$10^y\equiv 1,$$

此处 y 可为任一正整数.于是

$$a\cdot 10^y\equiv a,$$

这里，a 亦为任一正整数，它可以按照我们的需求，任取十个数

码之一. 任一正整数 N,按十进制记法,可写为

$$N=(a\cdot 10^{y})+(b\cdot 10^{y-1})+(c\cdot 10^{y-2})+\cdots+(q\cdot 10^{1})+r,$$

而对模 9 来说,有:

$$a\cdot 10^{y}\equiv a,$$
$$b\cdot 10^{y-1}\equiv b,$$
$$c\cdot 10^{y-2}\equiv c,$$
$$\cdots\cdots$$
$$q\cdot 10^{1}\equiv q,$$
$$r\equiv r.$$

把这些同余式相加,便得

$$N\equiv a+b+\cdots+q+r \mod 9. \qquad [56]$$

这就意味着,一个数与其数码和有着相同的九余数.

* * *

下面的问题可以测试一下读者对数码位值概念的掌握程度. 你能否猜到哪一个和数更大些? †[①]

1	2	3	4	5	6	7	8	9									1
1	2	3	4	5	6	7	8									2	1
1	2	3	4	5	6	7									3	2	1
1	2	3	4	5	6									4	3	2	1
1	2	3	4	5									5	4	3	2	1
1	2	3	4									6	5	4	3	2	1
1	2	3									7	6	5	4	3	2	1
1	2									8	7	6	5	4	3	2	1
1									9	8	7	6	5	4	3	2	1

* * *

卢卡在其著作《数学娱乐》中,列出了下列奇妙表格:

① 带有†号的问题在第 26 章中有解答. —— 原注.

$$
\begin{aligned}
1 \cdot 9 + 2 &= 11 \\
12 \cdot 9 + 3 &= 111 \\
123 \cdot 9 + 4 &= 1111 \\
1234 \cdot 9 + 5 &= 11111 \\
12345 \cdot 9 + 6 &= 111111 \\
123456 \cdot 9 + 7 &= 1111111 \\
1234567 \cdot 9 + 8 &= 11111111 \\
12345678 \cdot 9 + 9 &= 111111111 \\
123456789 \cdot 9 + 10 &= 1111111111
\end{aligned}
$$

表 23 神奇的数字宝塔

如果我们把等式左边的一般项(第 n 项)改写为

[57]

$$(10^{n-1} + 2 \cdot 10^{n-2} + 3 \cdot 10^{n-3} + \cdots + r \cdot 10^{n-r} + \cdots + n) \times (10 - 1) + (n + 1),$$

上述现象的底蕴即显而易见了. 因为,在把括弧乘出并化简后,即得:

$$10^n + 10^{n-1} + 10^{n-2} + 10^{n-3} + \cdots + 10 + 1 = (10^{n+1} - 1)/9.$$

如用普通的书写法,那就是 1 重复出现 $(n+1)$ 次.

* * *

$$
\begin{aligned}
9 \cdot 9 + 7 &= 88 \\
98 \cdot 9 + 6 &= 888 \\
987 \cdot 9 + 5 &= 8888 \\
9876 \cdot 9 + 4 &= 88888 \\
98765 \cdot 9 + 3 &= 888888 \\
987654 \cdot 9 + 2 &= 8888888 \\
9876543 \cdot 9 + 1 &= 88888888 \\
98765432 \cdot 9 + 0 &= 888888888
\end{aligned}
$$

表 24 神奇的数字宝塔

这里,第 n 项表达式为:

$$[9 \cdot 10^{n-1} + 8 \cdot 10^{n-2} + 7 \cdot 10^{n-3} + \cdots + r \cdot 10^{n-10+r} + \cdots + (10 - n)] \times (10 - 1) + (8 - n).$$

化简后,即得

$$9\cdot 10^n-(10^{n-1}+10^{n-2}+10^{n-3}+\cdots+10+1)-1$$
$$=8(10^{n+1}-1)/9.$$

由于$(10^{n+1}-1)/9$便是把1连写$(n+1)$遍，此数再乘上8，就得到所需乘积. 若$n=5$，即有

$$8(10^6-1)/9=8\cdot 111111=888888.$$

*　　　*　　　*

1 • 8+1 = 9
12 • 8+2 = 98
123 • 8+3 = 987
1234 • 8+4 = 9876
12345 • 8+5 = 98765
123456 • 8+6 = 987654
1234567 • 8+7 = 9876543
12345678 • 8+8 = 98765432
123456789 • 8+9 = 987654321

表 25　神奇的数字宝塔

[58]

987654321 • 9 = 888888888 9
987654321 • 18 = 1 777777777 8
987654321 • 27 = 2 666666666 7
987654321 • 36 = 3 555555555 6
987654321 • 45 = 4 444444444 5
987654321 • 54 = 5 333333333 4
987654321 • 63 = 6 222222222 3
987654321 • 72 = 7 111111111 2
987654321 • 81 = 8 000000000 1

表 26　奇妙的数型

12345679 • 9 = 111111111
12345679 • 18 = 222222222
12345679 • 27 = 333333333
12345679 • 36 = 444444444
12345679 • 45 = 555555555
12345679 • 54 = 666666666
12345679 • 63 = 777777777
12345679 • 72 = 888888888
12345679 • 81 = 999999999

表 27　奇妙的数型

数 12345679 可记为$(10^9-1)/81$，用 9 的倍数 $9K$ 去乘它，可以得出

$$9K(10^9-1)/81 = K(10^9-1)/9 = K(111111111);$$

当 K 相继取值 1，2，3，…时，我们即可得出表中的结果.

可利用这种关系来表演一个戏法. 先写下 12345679，再请人挑选一个他最喜爱的数字. 然后你通过心算，把他选定的数乘以 9，将乘积写在下面. 此时，你可对他说，既然他喜爱那个数字，眼下就有一大堆数字可供应他. 接着，你把两数相乘，戏剧性效果就出现了. 譬如说他选定的数是 4，那么，把 12345679 乘以 36，结果便是 444444444.

另一个例子是

$$\frac{1}{891} = \left(\frac{1}{81}\right)\left(\frac{1}{11}\right) = 0.00112233445566778 9\cdots.$$

如乘以 99，即得

[59] $$\frac{99}{891} = \frac{1}{9} = 0.11111\cdots.$$

问人家喜爱什么数字，设他的回答是 7，那就用心算把 99 乘以 7，得出 693. 把上述的位数很多的数乘以 693，即相当于求下列分数值

$$\frac{693}{891} = \frac{7}{9} = 0.77777\cdots.$$

$\frac{1}{81}$这个分数还可以为我们作更多表演（为了书写简单起见，下文略去小数点）.

$$1/81 = 1/81 = 12345679\cdots,$$
$$3/81 = 1/27 = 37037037\cdots,$$
$$6/81 = 2/27 = 74074074\cdots,$$

$$12/81 = 4/27 = 148148148\cdots,$$
$$15/81 = 5/27 = 185185185\cdots,$$
$$66/81 = 22/27 = 814814814\cdots.$$

只须记住$\frac{3}{81}=\frac{1}{27}$，其他结果都可作为其简单整倍数而导出.

由$\frac{1}{891}=\frac{1}{81\cdot 11}=1122334455667789$，我们得出

$$\frac{33}{891}=\frac{1}{27},$$

从而有，

$$1122334455667789 \cdot 33 = 37037037037037037,$$
$$1122334455667789 \cdot 3 = 3367003367003367.$$

读者们也许乐于找出 111222333444555666777889 所对应的分数吧.†

此时我们有

$$111222333444555666777889 \cdot 3 = 333667000333667000333667,$$
$$111222333444555666777889 \cdot 333 = 37037037037037037037037037037.$$

*　　　*　　　*

以下一则是提供给孩子们的：

$3 \cdot 37 = 111$	而	$1+1+1 = 3$
$6 \cdot 37 = 222$	而	$2+2+2 = 6$
$9 \cdot 37 = 333$	而	$3+3+3 = 9$
$12 \cdot 37 = 444$	而	$4+4+4 = 12$
$15 \cdot 37 = 555$	而	$5+5+5 = 15$
$18 \cdot 37 = 666$	而	$6+6+6 = 18$
$21 \cdot 37 = 777$	而	$7+7+7 = 21$
$24 \cdot 37 = 888$	而	$8+8+8 = 24$
$27 \cdot 37 = 999$	而	$9+9+9 = 27$

表 28　奇妙的数型

[60] * * *

以下一些表格选自席尔金(F. B. Selkin)的一篇论文,原载《师范学院教学资料》第12卷第68页.

1·1	=	1
11·11	=	121
111·111	=	12321
1111·1111	=	1234321
11111·11111	=	123454321
111111·111111	=	12345654321
1111111·1111111	=	1234567654321
11111111·11111111	=	123456787654321
111111111·111111111	=	12345678987654321

表 29 神奇的数字宝塔

7·7 = 49
67·67 = 4489
667·667 = 444889
6667·6667 = 44448889
66667·66667 = 4444488889
666667·666667 = 444444888889
6666667·6666667 = 44444448888889
等等

表 30 神奇的数字宝塔

4·4 = 16
34·34 = 1156
334·334 = 111556
3334·3334 = 11115556
33334·33334 = 1111155556
等等

表 31 神奇的数字宝塔

9·9 = 81
99·99 = 9801
999·999 = 998001
9999·9999 = 99980001
99999·99999 = 9999800001
999999·999999 = 999998000001
9999999·9999999 = 99999980000001
等等

[61] 表 32 神奇的数字宝塔

$$\begin{aligned}7\cdot 9 &= 63\\ 77\cdot 99 &= 7623\\ 777\cdot 999 &= 776223\\ 7777\cdot 9999 &= 77762223\\ 77777\cdot 99999 &= 7777622223\\ 777777\cdot 999999 &= 777776222223\end{aligned}$$

等等

表 33 神奇的数字宝塔

*　　　*　　　*

1837 年版的一本德-美代数课本列出了下面的模式：

$$\begin{aligned}1\cdot 7+3 &= 10\\ 14\cdot 7+2 &= 100\\ 142\cdot 7+6 &= 1000\\ 1428\cdot 7+4 &= 10000\\ 14285\cdot 7+5 &= 100000\\ 142857\cdot 7+1 &= 1000000\\ 1428571\cdot 7+3 &= 10000000\\ 14285714\cdot 7+2 &= 100000000\\ 142857142\cdot 7+6 &= 1000000000\\ 1428571428\cdot 7+4 &= 10000000000\\ 14285714285\cdot 7+5 &= 100000000000\\ 142857142857\cdot 7+1 &= 1000000000000\end{aligned}$$

表 34 神奇的数字宝塔

这显然来源于$\frac{1}{7}$的循环节.

*　　　*　　　*

下列关系式很有趣，未给出证明的这些结果可以提供给读者作为练习的素材.

$$\begin{aligned}7\cdot 15873 &= 111111,\\ 14\cdot 15873 &= 222222,\\ 21\cdot 15873 &= 333333,\\ 28\cdot 15873 &= 444444,\end{aligned}$$

等等.

请问：何以如此？† 此外还有

$$91\cdot 1221 = 111\ 111,$$

以及

$$900991 \cdot 123321 = 111\ 111\ 111\ 111.^{\dagger}$$

[62] * * *

用 1001 去乘一个三位数，其乘积是该三位数以及此数再重复一遍的六位数.例如

$$352 \cdot 1001 = 352352,$$
$$621 \cdot 1001 = 621621.$$

此关系式可用于速算表演.数

$$1001 = 7 \cdot 11 \cdot 13 = 7 \cdot 143.$$

你请人家随便挑一个三位数，例如 352.此时你把它乘上 7，心算出 2464，以它作被乘数，然后在它下边写上乘数 143，一下子就得出乘积 352352.

类似的结果也可从 $10001 = 73 \cdot 137$ 与 $100001 = 11 \cdot 9091$ 导出.例如一个四位数 7319 相继乘以 137 与 73，其积便是 73197319，而一个五位数乘以 11 与 9091 之后就得出原数再重复一遍的十位数.

* * *

有个很普通的戏法，其变种多得不计其数.请别人写出一个三位数，接着把该数逆序书写，然后两数相减(大减小)，把所得之差也逆序书写，然后再相加，这时你无需外加任何信息，即可断定结果必然是 1089.例如所选之数是 173，用 371 减去它，得 198，逆序书写得 891，后两数一加，其和便是 1089.

有个市井故事——老处女与猫，巧妙地利用了上述原理.想为其宠物取个名字却不太清楚猫的性别，又羞于向友朋启齿，于是她决定去找术数家(即数字算命人).她手足震颤，战战兢兢，转弯抹角地提出了问题，巫师对她说，数字占卜术能轻而易举地判别猫的性别，但要求她随便提几个候选名字.老处女羞答答地说，为了纪念一个远方的密友，如是一只雌猫的话，可取"埃玛"

(Emma)这个名字；若是雄猫，那就取名为“托-托”(Toy-Toy)．巫师听了，装模作样地写下了这两个名字，并在其下面写了10个数目字：

EMMA	TOY	TOY
9 8 7 6	5 4 3	2 1 0

[63]

接着，他开腔了：“夫人，在这些事情上，潜意识起着无可替代的作用．自然界的阴、阳两大要素必须按比例掺合．现在请你在“EMMA”这组中挑出一个数码，而在“Toy-Toy”一组中挑出两个数码，你愿不愿意？”她依言行事，小心翼翼地在第一组中挑出7，第二组中挑出3与2(其实，随便她挑什么数码，结果都一样)．巫师写下732，并把237写在下面，两数相减，再把差数的逆序数求出来，与差数相加，就得到了1089．“太太，”巫师说，“一切动物都有它们的性数，而猫是20．让我们把结果乘上20，这就得出21780，通过这种整数的神秘呼叫，让我们准备接受其答案吧．第一个数码2相当于猫的名字的第一字母T，然后，1相当于O，7是M，8是M，0是Y．”接着，他戏剧性地作了结论：“太太，你的这只猫，就叫它‘汤咪’(TOMMY)吧！”

上文提到，逆序操作的结果可得出1089，这是不难证明的．任何一个三位数可记为$a\cdot10^2+b\cdot10+c$，其逆序数为$c\cdot10^2+b\cdot10+a$．假定先写较大的数，即$a>c$．相减时在个位与十位上都要从上一位商借．这意味着出借者要减少1，而借入者要加上10．故可记录如下：

$$
\begin{array}{rlll}
 & (a-1)\cdot10^2+ & (b+10-1)\cdot10+ & (c+10) \\
 & c\cdot10^2+ & b\cdot10+ & a \\
\hline
\text{差数}= & (a-1-c)\cdot10^2+ & 9\cdot10+c+10-a & \\
\text{差的逆序数}= & (c+10-a)\cdot10^2+ & 9\cdot10+a-1-c & \\
\hline
\text{再相加，其结果是} & 9\cdot10^2+ & 180+9=1089. &
\end{array}
$$

*　　*　　*

一些学生及热心自学者发现了数的某些规律而沾沾自喜，他们自以为在数学里引发了一场革命，但实际上却不过是数码9的一些初等性质而已. 绝大多数情况下，此类结果非常肤浅，用同余式或其他手段即可轻易导出. 但人们毕竟也应记住，数论或许是唯一的数学分支，足以使阅历虽浅但充满好奇与精力充沛者能在此领域中有所作为，从中发现一些新鲜事物.

[64] * * *

数 9 具有一个“神奇”性质：除去 2 与 5 之外，任一素数均能整除长度无限的，各位数字统统由 9 构成的正整数. 例如 999 能被 39 整除，而 999999 与 999999999 亦然，如此等等. 另外，41 能整除 99999 以及任意 5K 个 9，而 73 可整除 99999999. 只要四个 9 即可被 101 整除，但若想被 97 整除，没有 96 个 9 是不行的. 素数 271 可以整除 99999，但前一个素数 269 却需要 268 个 9 才行. 素数 4649 可整除 9999999，但下一个素数 4651 则非有 4650 个 9 串成一个长链不可. 只要 10 个 9 即可对付 9091，但需有 9102 个 9 才能对付 9103. 当然，20，30，40，50，…个 9 也是能被 9091 除尽的，但在考虑被 9103 整除的情况时，除了 9102 个 9 串接能被它整除之外，下一次还得有 9102 个 9，即一共 18204 个 9 才行.

证明其实比人们所预期的要简单. 眼光敏锐的读者会发现，这一性质不仅对数码 9，对其他清一色反复出现的数码同样也成立. †

$12 \cdot 483 = 5796$ $27 \cdot 198 = 5346$

$42 \cdot 138 = 5796$ $39 \cdot 186 = 7254$

$18 \cdot 297 = 5346$ $48 \cdot 159 = 7632$

$28 \cdot 157 = 4396$

$4 \cdot 1738 = 6952$

$4 \cdot 1963 = 7852$

表 35 奇异乘法，九个数码全都用上了

*　　　*　　　*

上面的表格说明，如何通过巧妙安排，使乘法等式中不重不漏地出现全部九个数码.

51249876 与 3（所有的数码都只用过一次）的积是 153749628，其中全部九个数码都出现，且无重复. 另外还有：

$$16583742 \cdot 9 = 149253678,$$
$$32547891 \cdot 6 = 195287346.$$

*　　　*　　　*

用 5 去乘 142857 时，只要把 7 从最右一位移到最左，即可得出乘积 714285.

数 3529411764705882 乘上 2 再除以 3，也只要把末位的 2 移到最左面去，即可得出正确结果. [65]

*　　　*　　　*

另外还有一些有趣的数码问题，请看第 25 章.

参考文献

Brooks, E. *Philosophy of Arithmetic*. Lancaster, Pa.: Normal Publishing Co., 1880.

Jones, S. I. *Mathematical Nuts*. Nashville, Tenn.: S. I. Jones, 1932.

Lucas, E. *Récréations Mathématiques*. Paris: Gauthier-Villars et Cie., 1882.

Merrill, H. A. *Mathematical Excursions*. New York: Dover Publications, Inc., 1957.

Selkin, F. B. "Number Games Bordering on Arithmetic and Algebra," *Teachers College Record*, **13**(1912), 68.

Simons, L. G. "A German-American Algebra of 1837," *Scripta Mathematica*, **1**(1932), 29.

Smith, D. E. *Wonderful Wonders of* 1, 2, 3. New York: McFarlane, Ward, McFarlane, 1937.

White, W. F. *Scrap Book of Elementary Mathematics.* Chicago: Open Court Publishing Co., 1910.

[66]

第9章 记数法乱弹琴

"一乘六得六；二乘六为十五；三乘六得二十四；四乘六得三十三；五乘六得四十二；六乘六是五十一；而'十'乘六为六十."

多么奇怪的乘法表！但若我们记数制的"基"用 7 来取代 10 的话，背诵起乘法的"六六表"(而不是"九九表")来就是这种样子. 在这一记数制中见不到 7，8，9；6 以后就一直跳到两位数 10，它意味着 7(十进制). 所以，在本节开头的记法中，"十"便相当于 7 个单位.

要孩子们记住乘法表是相当困难的，在我们的十进位记数制中掌握乘法运算需要大量练习. 在 $2\times4=8$ 这问题上，直觉帮不了我们什么忙. 我们觉得那是理所当然的. 如果在孩童时期我们所学的是七进位乘法 $2\times4=11$，那么它也很"自然"，并不会比 $2\times4=8$ 更为怪异.

在七进制中我们如下计数 1，2，3，4，5，6，10，11，12，13，14，15，16，20，21，22，23，24，25，26，30，等等，然后会遇到 61，62，63，64，65，66，100，等等. 第一个二位数不妨随便起个名字；为了避免混淆，可以叫它"十"，但也可叫"七"或者"权". 七进位记数制中的某数并不意味着它是十进制中该数的十分之七. 事实上，7 的乘幂对应于 10 的乘幂. 在十进制中，数 329 的意思是$3\cdot10^2+2\cdot10+9$. 为了将它转变到以 7 为"基"的数制，我们连续用 7 去除并记下余数. 亦即 $329\div7=47$，无余数；$47\div7=6$，余 5；$6\div7=0$，余 6. 逆序书写余数，相当于 7 的乘幂的对应系数，于是十

进制数 329 即相当于七进数 650. 类似地，将 5218 改写为“我们的”记数制中的数，可这样做：

被除数	余数
7 | 5 2 1 8	
7 | 7 4 5	3
7 | 1 0 6	3
7 | 1 5	1
7 | 2	1
0	2

[67]

它是七进数 21133. 要想把七进数 21133 返回十进制，则应把每位数码视为 7 的乘幂的系数并进行如下计算. 例如：

$$2\cdot 7^4+1\cdot 7^3+1\cdot 7^2+3\cdot 7^1+3$$
$$=4802+343+49+21+3=5218.$$

上面所说的连续用 7 去除的办法不过是一种方便的办法，用以决定该数中含有的 7 的最高次幂，接下来是次高乘幂，如此等等，还包括它们的系数. 因此，我们可以这样说：“$7^5=16807$ 是太大了；$7^4=2401$ 在数 5218 中包含了二度；在余数 $416=5218-2\cdot 2401$ 中，$7^3=343$ 被包含了一次；在新的余数 73 中 $7^2=49$ 被包含了一次；而在余数 24 中包含了三个 7^1；最后的余数相当于末位数是 3.”

在七进位世界里，我们要学习的乘法表如下：

1 × 1 = 1	1 × 2 = 2	1 × 3 = 3
2 × 1 = 2	2 × 2 = 4	2 × 3 = 6
3 × 1 = 3	3 × 2 = 6	3 × 3 = 12
4 × 1 = 4	4 × 2 = 11	4 × 3 = 15
5 × 1 = 5	5 × 2 = 13	5 × 3 = 21
6 × 1 = 6	6 × 2 = 15	6 × 3 = 24
1 × 4 = 4	1 × 5 = 5	1 × 6 = 6
2 × 4 = 11	2 × 5 = 13	2 × 6 = 15
3 × 4 = 15	3 × 5 = 21	3 × 6 = 24
4 × 4 = 22	4 × 5 = 26	4 × 6 = 33
5 × 4 = 26	5 × 5 = 34	5 × 6 = 42
6 × 4 = 33	6 × 5 = 42	6 × 6 = 51

表 36　基数为 7 的乘法表

现在让我们试做一下加法与乘法.相加时要记住6的后面是10;16的后面是20;26的后面是30;……;66的后面便是100了.下面的加法算式显而易见,其中出现的数都已经是七进数,其位值是7的乘幂,而非10的乘幂.

[68]

我们像通常一样做加法,但对于每个7的倍数,便当成七进制中的"十"并进上一位,而将余数写在本位.应注意数码7,8,9是绝对不出现的.

```
   2514
   5603
   2051
+  6643
  23444
```

只要参照乘法表,做起乘法来也很容易(如果我们想撇开表格,那就得记熟口诀,以提高速度,发展运算技巧),正如我们在童年时期利用"九九表"做乘法一样.

```
      6542
×     3105
     46003
    65420
 26256
 30322203
```

在这里,积的第一行值得特别为之作一些说明.按乘法表,我们说:"5乘2等于13,写3进1;5乘4等于26,加上进过来的1,等于30,于是写0进3;5乘5等于34,加上进位的3,等于40,于是写0进4;5乘6等于42,加上进位的4,故得46."(假定进位的是5,那样的话42加5便等于50.)

*　　*　　*

无须多言,此外还有其他"基数"的进位制度——有些人主张采用12进位制.这时,需发明两个新的记号来代表10与11,

因为那时，只有在比 10 再大 2 的时候才能启用二位数.

由于数字计算机的广泛使用，近年来人们很熟悉二进位记数法. 这时，任一正整数都只能用 0 与 1 来表示. 例如，为了把数 54 转化为二进数，可用 2 连续去除此数直到整除无余，这时的余数就给出相应的二进数. 即：[69]

被除数	余数
2 | 54	
2 | 27	0
2 | 13	1
2 | 6	1
2 | 3	0
2 | 1	1
0	1

故十进数 54 相当于二进数 110110.

由于二进位记数法中只用两个记号 0 与 1，这就使它与下面两种物理系统建立起一一对应关系：(1)继电器触点的闭或开；(2)电源供应终端的“正”或“负”. 二进制记数法之所以在数字计算机中用得如此广泛，其理由即在于此.

上述办法难免有点混淆不清，不妨请你想一想，十进制小数或分数与非十进制的分数应怎样互相转化. 建议读者去参阅一下有关课本，例如克里斯多(G. Chrystal)所著的《代数学》①，该书对此课题有进一步的阐述.

一个数用二进位记数法表达时，2 的方幂的系数只能是 0 或 1；这一事实意味着，任何整数都可表达成 2 的各次方幂之和，而每个方幂的系数都为 1. 例如 $54=2^5+2^4+2^2+2$.

就三进位记数法而言，系数是 0，1 或 2，如果我们把 2 写成

---

① G. Chrystal, Textbook of Algebra(共有二卷，纽约市 Dover 出版公司，1961 年版). ——原注.

(3－1)，这就意味着，任一正整数都可表达为3的若干个乘幂之和或差. 例如数65在三进制里对应于：

$$2\cdot 3^3+1\cdot 3^2+2\cdot 3^0=(3-1)3^3+1\cdot 3^2+(3-1)3^0$$
$$=3^4-3^3+3^2+3^1-3^0.$$

有名的天平称重问题与最后提到的表示法则具有密切联系. 由于2的若干个乘幂之和可用以表示任何整数，因此我们可以用1，2，4，8，16等磅的砝码在天平上称出任何整数重量. 但是，3的乘幂工作起来同样好——事实上更好些——如果允许在天平的两只盘子里都能放砝码的话. 此事其实对应于加或减3的幂. 只要利用1，3，9，27磅四种砝码，就可以称出直到40磅为止的任何整数重量，只要再加上一只81磅的砝码，便可称到121磅，如此等等. [70]

*　　*　　*

有个故事提到一位只会做加法以及乘2与除以2的农民，尽管他的知识装备如此可怜巴巴，但他却能做任何两个数的乘法. 例如，他要算89×107，首先，他把它们写在二列数字的开头，然后把第一数反复地除以2，并相继书写其结果. 相除时，余数不予考虑. 第二列的数字则反复乘上2，也同样一一书写出来. 最后，他只是把第二列中对应于第一列中奇数的那些数目(下面我们用一个星号表示)加起来，而正确答数居然呈现出来了. 以下的例子足以充分说明这种办法.

89*	107
44	214
22	428
11*	856
5*	1712
2	3424
1*	6848

乘积　$89\cdot 107=107+856+1712+6848=9523.$

这一做法的理由当然不难理解.相继用 2 去除 89 实际上就是在把它表示为二进数(就像对 54 所做的那样),只是第一列中的奇数才会留下余数 1,而后者正是决定 2 的乘幂的系数.所以,余数是 1,0,0,1,1,0,1,把它们逆序地记录为 2 的乘幂,亦即

$$89 = 1\cdot 2^6+0\cdot 2^5+1\cdot 2^4+1\cdot 2^3+0\cdot 2^2+0\cdot 2^1+1\cdot 2^0.$$

于是,

$$\begin{aligned}107\cdot 89 &= 107\cdot 2^6 + 107\cdot 2^4 + 107\cdot 2^3 + 107\cdot 2^0\\ &= 6848 + 1712 + 856 + 107 = 9523.\end{aligned}$$

[71]

参考文献

Barlow, P. *Theory of Numbers*. London: J. Johnson & Co., 1811.

Chrystal, G. *Textbook of Algebra*. 2 vols. New York: Dover Publications, Inc., 1961.

[72]

第10章 循环到无穷

在小学里，小数（十进分数）是很头痛的东西，可是支配它们的原理与性质却很有趣，这在少年儿童的心目中是很难梦想到的. 让我们先来复习一下某些简单分数.

$$\frac{1}{3}=0.333\cdots \qquad \frac{1}{7}=0.142857142857\cdots$$

$$\frac{1}{4}=0.25 \qquad \frac{1}{9}=0.111\cdots$$

$$\frac{1}{5}=0.2 \qquad \frac{1}{11}=0.0909\cdots$$

$$\frac{1}{6}=0.1666\cdots \qquad \frac{1}{13}=0.076923076923\cdots\cdots$$

为什么有些小数是有限的，有些小数的第一位数字即无限重复，有些在前几位小数之后开始循环，还有一些（例如$\frac{1}{7}$，$\frac{1}{11}$，$\frac{1}{13}$）则周而复始地有好几位循环数字？绝大多数读者可能已经知道这样一个事实：若某一整数的倒数可表达为有限小数，其必要条件是该整数只含有 2，5 的方幂，或兼而有之. 在不超过 100 的正整数中，这类数字是 2，4，5，8，10，16，20，25，32，40，50，64，80，100. 这些数都只包含 2 与 5 的方幂，因而它们的倒数均为有限小数. 除此之外，就没有了. 举一个例子：$\frac{1}{64}=0.015625$.

倒是在此之外的整数，可以提供小数方面的娱乐性材料. 为

了理解循环节，较方便的办法是用给定整数去除 10 的一个乘幂. 例如对 7 的倒数，我们考虑 $10^r/7$. 由费马小定理 $10^{p-1} \equiv 1 \bmod p$，也就是说，我们需将 10 自乘到不大于 $p-1$ 的某个指数，以使得它在被素数 p 去除时余数是 1. 有时，指数可能是一个较小的数，这种最小指数必为 $p-1$ 的因子. 如果 $10^e \equiv 1 \bmod p$，此处e是给出余数1的最小指数，则e表示p的倒数表为小数时，其循环节的位数.

[73]

由费马小定理，$10^2 \equiv 1 \bmod 3$，但较小指数 1 即已有性质 $10^1 \equiv 1 \bmod 3$，因而 $\frac{1}{3}$ 在小数第一位就开始循环，事实上$\frac{1}{3}=0.333\cdots$. 类似地 $10^6 \equiv 1 \bmod 7$，但此时小于 6 的指数将不能使同余式成立，故知$\frac{1}{7}$的循环节有六位，而实际上$\frac{1}{7}=0.142857142857\cdots$. 当余数为 1 时要出现周而复始的情况，因为开始时被除数是 1，此时，第七次的余数将也是 1. 此外，$10^{10} \equiv 1 \bmod 11$，但 $10^2 \equiv 1 \bmod 11$，所以$\frac{1}{11}$的循环节有二位，而实际上$\frac{1}{11}=0.0909\cdots$.

继续进到较大素数，尽管 $10^{12} \equiv 1 \bmod 13$，但能使同余式成立的最小指数为 6，从而 $\frac{1}{13}$ 的循环节有六位，即 $\frac{1}{13}=0.076923\ 076923\cdots$. 对素数 17 来说，必需把 10 升高到 16 次方才能使余数为 1. 10 称为数 17 的一个原根，而 $\frac{1}{17}=0.0588235294117647\cdots$，且循环节从 0 开始. 同样，10 也是 19 的一个原根，故而$\frac{1}{19}$的循环节有 18 位. 表 37 给出了 10^e 除以素数 p 时余 1 的最小指数 e，从而表示$\frac{1}{p}$化成小数时循环节的位数. 数 10 被说成“属于 e，模 p.” 值得注意的是，在 1 与 100 之

间的23个奇素数中，10只是其中九个素数的原根，表中用† †号表示. 小于100的最大素数为97，而10是97的原根，从而$\frac{1}{97}$必须进行到96位小数才能出现循环！如果这能算是很大工作量的一桩事情，那么请想一想一个姓赫德逊(W. H. H. Hudson)的人，他竟然不厌其烦地算出了$\frac{1}{1861}$的1860位循环节，还有一个威廉·向克斯(William Shanks)，他算出了$\frac{1}{17389}$中的17388位循环节.

1863年，苏非德(Suffield)与伦恩(Lunn)在苏氏认为是他发明的一种综合除法"新"方法的解说中，算出了$\frac{1}{7699}$的7698位循环节. 但法国数学家傅利叶(Fourier)早在19世纪上半叶就已发现了此种方法，其后又被多次重新发现.《圣经·传道书》的作者写道："太阳底下没有新事物." 现在已经完全弄清楚：何

素数 p	最小指数 e	素数 p	最小指数 e
3	1	47† †	46
7† † [1]	6	53	13
11	2	59† †	58
13	6	61† †	60
17† †	16	67	33
19† †	18	71	35
23† †	22	73	8
29† †	28	79	13
31	15	83	41
37	3	89	44
41	5	97† †	96
43	21		

表37 由素数3至97[2]，数10所属之指数

① 10是带† †号素数的原根.——原注.

② e是10的最小幂指数以使10^e-1能被素数p整除.——原注.

以$\frac{1}{2}$，$\frac{1}{4}$，$\frac{1}{5}$的等价物是有限小数，$\frac{1}{3}$的循环节有一位，$\frac{1}{7}$有六位，何以一般$\frac{1}{p}$有e位，其中e是使$10^e \equiv 1 \bmod p$成立的最小正整数.

[74]

表 37 仅不过是一张庞大无比的表格的开头部分，有许多计算者竟然愿意献出一生的大部分时光从事这项工作而别无报酬. 威廉·向克斯真是一个精力充沛的幽灵(是他把圆周率算到 707 位小数，但只正确到前面 528 位)，他居然把 120000 以下所有素数的倒数统统算了出来. 我们已经知道$10^{96} \equiv 1 \bmod 97$，并懂得如有较小的指数能使该同余式成立，则这些指数必为 96 的因子. 因此，必须检查10^2，10^3，10^4，10^6，10^8，10^{12}，10^{16}，10^{24}，10^{32}，10^{48}在被 97 去除时能否得出余数 1. 注意：这仅仅是一个素数的工作量. 请想一想，把所有 120000 以下的素数统统算一下要花费多少精力. 当然，其中有许多窍门，向克斯也曾参考过前人已编出的较小表格，但即便如此，工程依旧十分庞大. 然而，在他身后的研究者，例如艾伦·克宁汉(Allan Cunningham)竟能把向克斯的计算全部复核一遍!

人们对这些在地球的各个角落里作出不懈努力的人感到不可理解，他们在一种难以表达的冲动下打算为世上小小的知识宝库添砖加瓦. 如果人们走进图书馆里的冷角落，一头投入尘封的卷帙，一页一页地走近那些由德国人、法国人、意大利人、美国人、英国人精心编制的数字表格，一种超越国界与偏见、歧视的科学同志感情就会从他的心底里油然而生. 例如，翻阅 1873 年《伦敦皇家学会公报》第 22 卷，看看向克斯所作的计算①，你就会得到这种启示.

[75]

① 如果读者有机会查阅这些文献，他将发现皇家学会印制的表格截止于素数 29989，但皇家学会的成就记录则保存了直到 120000 为止的作者手稿. ——原注.

* * *

1/7 = 0.142 857…	1/17 = 0.05882352 94117647…
2/7 = 0.285 714…	2/17 = 0.11764705 88235294…
3/7 = 0.428 571…	3/17 = 0.17647058 82352941…
4/7 = 0.571 428…	14/17 = 0.82352941 17647058…
5/7 = 0.714 285…	15/17 = 0.88235294 11764705…
6/7 = 0.857 142…	16/17 = 0.94117647 05882352…

表 38 $\frac{a}{7}$与$\frac{a}{17}$的小数循环节

表 38 的分数表现出一个奇妙性质. $\frac{1}{7}$的每一整数倍仍是同样六个数码的重新轮转. 对$\frac{1}{17}$的 16 个倍数来说也有类似的性质. 对于以 10 为原根的一切素数的倒数都是如此,例如$\frac{1}{19}$,$\frac{1}{23}$,$\frac{1}{29}$等等.

由于 p 为奇素数,从而 $p-1$ 是偶数,故当 10 为原根时,循环节的 $p-1$ 位小数可以等分为两组. 值得注意的是两组中的对应数码之和恒等于 9;因而,如果我们已经求得了前一半循环节,那么只要用 9 减去对应数码,即能轻而易举地写出循环节的后一半.

此性质不光是对 10 为原根的一切素数成立,而且对循环节含有偶数位数码的任何素数也成立. 例如,13 的循环节有六位. 表 37 告诉我们,31,37,41,43,53,67,71,79 与 83 的循环节含有奇数位数码;因此,对这些素数而言,就无所谓半循环节. 但对 100 以下的其余数码来说,其循环节都是含有偶数位数码的,从而前、后两个半节的对应数码之和一定是 9.

合数的倒数即使其循环节含有偶数位数码,也未必具有这种半节互补性. 例如合数 403 的循环节有 30 位,亦即 [76] 002481389578163 771712158808933,但这两个半节并不互补. 这是由于 $403=31\cdot13$,而$\frac{1}{31}$的循环节含奇数位数码,从而影响

了结果. 另外的例子有$\frac{1}{21}$,$\frac{1}{33}$,$\frac{1}{39}$,$\frac{1}{51}$,分母上都有 3 这个因子,而$\frac{1}{3}$的循环节有着奇数位数码.

决定循环节的具体数字有许多办法. 较方便的是,在除法中出现较小余数时若已求出许多位数码,则可利用乘法,一下子写出后继的许多位数来. 例如,由于 10 是 97 的一个原根,故$\frac{1}{97}$有 96 位循环节. 先用普通除法进行计算,我们得出

$$\frac{1}{97}=0.01030927835\,\frac{5}{97}.$$

余数$\frac{5}{97}$正好是$\frac{1}{97}$的五倍,因此后继的 11 位数字肯定必是已求出的前 11 位数字的五倍,亦即 05154639175,而 $5\left(\frac{5}{97}\right)=\frac{25}{97}$是新的余数. 此时,分子又是一个较方便的乘数,因为乘上 25 即相当于乘 100(只要把小数点向右移两位)再除以 4. 对目前已经求得的 22 位数码执行此种运算,我们得到 1.03092783505154639175,后者在除以 4 后,便给出紧接于后的 22 位数码:2577319587628865979375,再附加一个余数 $25\cdot25=625$. 但是,

$$625/97=6\,\frac{43}{97},$$

故应在已算出的结果中加上 6,即把最后两位数码由 75 修改为 81,并对余数 43 继续作除法. 下面四个数码是实际执行 $43\div97$ 的结果,得 4432. 这时由于相当于半周期的 48 位数码都已求得,于是根据上述性质,后半周期马上即可一举求出. 总之,真正做除法只做了 15 次,96 位循环节便都求出来了. 全部循环节是:

$\frac{1}{97}$=0.010309278350515463917525773195876288659793814432
989690721649484536082474226804123711340206185567…

随后，又是 0103…卷土重来！ [77]

如果 10 不是 p 的一个原根，情况就有所不同.

第一组	第二组
1/13 = 0.076 923…	2/13 = 0.153 846…
3/13 = 0.230 769…	5/13 = 0.384 615…
4/13 = 0.307 692…	6/13 = 0.461 538…
9/13 = 0.692 307…	7/13 = 0.538 461…
10/13 = 0.769 230…	8/13 = 0.615 384…
12/13 = 0.923 076…	11/13 = 0.846 153…

表 39 $\frac{a}{13}$的循环节

这里有两组循环轮转的配置.在同一组中，同样六个数码像走马灯似地转圈子，但开头的数码不一样.如果 10“属于”更小的指数，即比 $p-1$ 的一半还小，则我们就有更多的组.譬如说，以 37 为分母的 36 个分数可分为 12 组，而每组都有不同数字在转圈子.12 组里头，每组都有三个分数，因为 $10^3 \equiv 1 \bmod 37$.但 $10^5 \equiv 1 \bmod 41$，因此对$\frac{1}{41}$的各整数倍来说，共可分为八组，而每组都有五名成员.

组别	分	数			
1	1/41=0.02439	10/41=0.24390	16/41=0.39024	18/41=0.43902	37/41=0.90243
2	2/41=0.04878	20/41=0.48780	32/41=0.78048	33/41=0.80487	36/41=0.87804
3	3/41=0.07317	7/41=0.17073	13/41=0.31707	29/41=0.70731	30/41=0.73170
4	4/41=0.09756	23/41=0.56097	25/41=0.60975	31/41=0.75609	40/41=0.97560
5	5/41=0.12195	8/41=0.19512	9/41=0.21951	21/41=0.51219	39/41=0.95121
6	6/41=0.14634	14/41=0.34146	17/41=0.41463	19/41=0.46341	26/41=0.63414
7	11/41=0.26829	12/41=0.29268	28/41=0.68292	34/41=0.82926	38/41=0.92682
8	15/41=0.36585	22/41=0.53658	24/41=0.58536	27/41=0.65853	35/41=0.85365

表 40 $\frac{a}{41}$的循环节

*　　　*　　　*

在小于 100 并用作真分数的分母的整数中，49 是一个较为独特的合数. 若 k 与 49 互质，则一切分数 $\frac{k}{49}$ 都是同样一些数码在轮转. 此种分数一共有 42 个，而每个分数都有 42 位循环节.

$$\frac{1}{49}=0.020408163265306122448\ 979591836734693877551\cdots$$

而

$$\frac{3}{49}=0.061224489795918367346\ 938775510204081632653\cdots$$

[78] 如此等等；其时，后一个分数的第二位数码是前一个分数的第 14 位数码. 具有此类性质的合数是大于 3 的单个素数的乘幂，而且 10 必须是该素数的一个原根.

*　　　*　　　*

在绝大多数情况下，一个素数乘数 p^a 的倒数的小数展开式，其循环节的位数 n 是 $r\cdot p^{a-1}$，这里的 r 是 $\frac{1}{p}$ 的循环节位数. 例如，$\frac{1}{11}$ 有着二位循环节 09，从而 $\frac{1}{11^2}$ 的循环节有 22 位；$\frac{1}{13}$ 的循环节有 6 位，于是 $\frac{1}{13^3}$ 的循环节有 $6\cdot 13^2=1014$ 位.

两个特别的例外是 $\frac{1}{9}=\frac{1}{3^2}$，它只有一位循环节，与 $\frac{1}{3}$ 的循环节位数相同；$\frac{1}{487^2}$ 的循环节有 486 位，与 $\frac{1}{487}$ 的情况一样. 在1000 以下的素数中，再也没有其他素数具有如此稀有的性质.

*　　　*　　　*

商与余数的循环轮转可以通过一种有趣的图解方式来显示，如图 2. 内环给出了 $\frac{1}{29}$ 的商，而外环给出了余数，开始于星号下面的一个数码，按顺时针方向前进.

1. 在商的圆周中，处于直径两端的数码，相加之和等于 9.

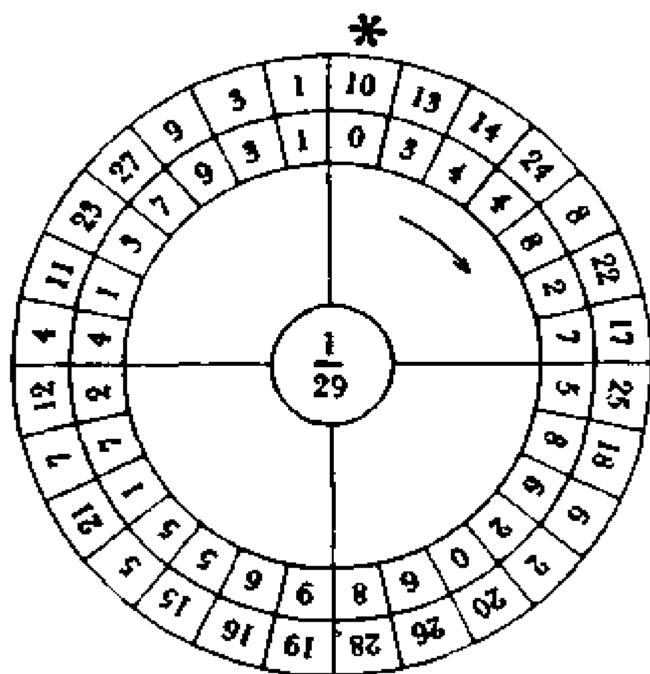


图 2　$\frac{1}{29}$的循环节

2. 处于直径两端的余数之和是 29.　[79]

3. 任一分数的循环节，例如$\frac{13}{29}$可用下法得出，首先在外环的余数圈中找到 13，在内环中，与之相应的商为 3. 然后，按顺时针方向，3 后面的下一个数码是 4，于是可以马上写出$\frac{13}{29}=0.44827586\cdots$.

通过制作这种圆形转盘，易于发现循环小数的一些其他性质.

*　　*　　*

有趣的是，可以按照一种完全不同于有限或循环的模式来写出小数. 我们在此只能略作介绍，因为它将把我们领得很远并沿着榛莽未辟的途径. 小数 0.101001000100001…遵循着以下规律：1 后面的 0 的个数每次都递增一个. 这个数字也可记为：

$$10^{-1}+10^{-3}+10^{-6}+10^{-10}+10^{-15}+\cdots+10^{-n(n+1)/2},$$

在此，指数为一个三角形数（参阅第 18 章），也就是一个等差数列之和. 还有

$$0.1101000100000001\cdots,$$

这里的 1 占据着第 1，2，4，8，16，…，2^n 位，相当于

$$10^{-1}+10^{-2}+10^{-4}+10^{-8}+\cdots+10^{-2^n}.$$

指数成一几何数列. 更复杂的是 0.11101010001010…，这里的 1 占据着第 1，2，3，5，7，11，13 位，亦即素数位置①. 然后是 0.123571113171923…，这是把素数按其自然顺序写下来的小数.

* * *

1823 年，亨利・戈德温（Henry Goodwyn）在伦敦印出一张 107 页长的表，给出了分母小于 1024，且与 10 互质的（包括素数与合数）一切分数的小数展开式. 例如$\frac{1}{127}$，$\frac{2}{127}$，$\frac{3}{127}$，等等全都算出来了. 如果这桩事情很受欢迎，戈德温无疑会编出更多表格来，然而公众对此缺乏热情. [80] 英国皇家学会在 1842 年购进了他的大量未刊行的分数手稿. 我们遗憾地指出，三十年之后，皇家学会的档案里根本找不到手稿记录，人们眼门前也许会出现一个幻像，某个毫无感情的扫街人在他的手推车装着的痰迹斑斑的废纸就是这位亨利・戈德温先生无效劳动的产物. 真是一度荣华，转眼即逝矣.

* * *

每个循环小数，不论它的循环节有多么长（但必须有终止的时候），都是一个有理数，即可表示为两个整数之商. 要求出这一分数（从分数化成小数的逆过程），我们可按下法进行：设 $N=$

---

① 西方数学书刊中常有人把 1 列作素数. 但我们则认为素数序列从 2 开始，1 不算素数. ——译者注.

0.076923076923…，循环节有六位.于是 $10^6N=76923.076923$…. 减去原数，即得 $999999N=76923$. 因此就有 $N=76923/999999=1/13$. 用另一个来再算一下，设 $N=0.0731707317\cdots$，循环节有五位.于是 $10^5N=7317.07317\cdots$，$10^5N-N=99999N=7317$. 所以

$$N=\frac{7317}{99999}=\frac{3}{41}.$$

参考文献

Bickmore, C. E. "On the Numerical Factors of a^n-1," *Messenger of Mathematics*, **25**(1895), 1.

Brooks, E. *Philosophy of Arithmetic*. Lancaster, Pa.: Normal Publishing Co., 1880.

Carmichael, R. D. *Theory of Numbers and Diophantine Analysis*. New York: Dover Publications, Inc., 1959.

Cunningham, A. *Haupt-Exponents, Residue Indices, Primitive Roots*. London: F. Hodgson, 1922.

——. "Note on Factors of (10^n-1)[Corrections]," *Messenger of Mathematics*, **33**(1903), 95.

Dickson, L. E. *History of the Theory of Numbers*. 3 vols. New York: Chelsea Publishing Co., 1950.

Escott, E. B. "Note Concerning the Numerical Factors of a^n-1," *Messenger of Mathematics*, **33**(1903), 49.

Glaisher, J. W. L. "On Circulating Decimals...," *Proceedings of the Cambridge Philosophical Society*, **3** (1876—1880), 185.

Guttman, S. "On Cyclic Numbers," *American Mathematical Monthly*, **41**(1934), 159.

Hardy, G. H. "An Introduction to the Theory of Numbers,"

Bulletin of the American Mathematical Society, **35**(1929),
[81] 778.

Lehmer, D. H. "Test for Primality by the Converse of Fermat's Theorem," *Bulletin of the American Mathematical Society*, **33**(1927),327.

Shanks, W. "On the Number of Figures in the Period of the Reciprocal of Every Prime Number Below 20000," *Proceedings of the Royal Society of London*, **22**(1873),200.

——. "Given the Number of Figures (Not Exceeding 100)in the Reciprocal of a Prime Number, to Determine the Prime Itself," *Proceedings of the Royal Society of London*, **22** (1873),381.

——. "On the Number of Figures in the Reciprocal of Every Prime Between 20000 and 30000," *Proceedings of the Royal Society of London*, **22**(1873),384.

White, W. F. *Scrap Book of Elementary Mathematics*. Chica-
[82] go: Open Court Publishing Co., 1910.

第11章　11111…111

由清一色的1重复有限多次所组成的数引起了人们很大的兴趣，为了求出它们的因子而花掉不少时间. 11 111 111 111 111 111 有没有因子，如果有的话，又是什么？这类数目可记为

$$10^{x}+10^{x-1}+10^{x-2}+\cdots+10^{2}+10+1,$$

利用通常的代数公式求此几何级数之和，可得$(10^{x+1}-1)/9$. 上述17位数可记为$(10^{17}-1)/9$，而问题转化为怎样找到形如$10^{y}-1$的数的因子.

有时把全由单独数码重复若干次而形成的数叫做清一色数. 为了方便起见，本书作者起用了一个专门名词"重一数"(重复的1)，以表示全然由清一色的1所组成之数.

当重一数的位数为素数时，作者就他所知，有关其因子情况的"最新"信息列举在表41之中. 我们将回忆得起，在第3章讨论梅桑数时已讲过，当y是合数时，此类二项式易于析出因子，因而仅当y为素数时，判别数的特性才有点困难. 讨论梅桑数用过的办法在分解$a^{x}-1$形式的数时也有帮助，只不过，现在的底数是10而不是2而已.

根据费马小定理，$a^{p-1}\equiv 1 \bmod p$. 当p为素数时，$p-1$是偶数. 因此定理不能直接应用到$a^{x}-1$形状的数，这是由于x为素数，故一般为奇数. 对梅桑数而言，底数是2，第3章中已讲过，若p为$8r+7$形状的数，则指数可以减半而不影响可除性，

[83] 即 $2^{4r+3}\equiv 1 \mod 8r+7$. 表 7 列出了形如 $4r+3$ 且不超过 257 的素数，以及相应的可整除 $2^{4r+3}-1$ 的素数 $8r+7$. 对底10而言，

y，一个素数	$R_y=(10^y-1)/9$ 的因子	性质
1	1	素数①
2	11	素数
3	3 • 37	合数
5	41 • 271	合数
7	239 • 4649	合数
11	21649 • 513239	合数
13	53 • 79 • 265371653	合数
17	2071723 • 5363222357	合数
19	1111111111111111111	素数
23	11111111111111111111111	素数
29	3191 • 16763 • 43037 • 62003 • 77843839397	合数
31	2791 • ?	合数
37	?	合数
41	83 • 1231 • ?	合数
43	173 • ?	合数
47	?	?
53	107 • ?	合数
59	?	?
61	733 • 4637 • ?	合数
67	493121 • ?	合数
71	?	?
73	?	?
79	317 • 6163 • 10271 • ?	合数
83	?	?
89	497867 • ?	合数
97	?	?

表 41 "重一数"的因子，

[84] **$R_y=111\cdots111(y\text{ 个 }1)=(10^y-1)/9$**

① 原文如此. 西方国家的数学书中，常有把 1 看作素数的，读者当明知其非，故仍维持原状，一律不改. ——译者注.

也有一个类似关系. 设 p 为素数，且具有以下形式 $40r\pm1$，$40r\pm3$，$40r\pm9$，$40r\pm13$ 之一，则有

$$10^{\frac{p-1}{2}}\equiv1 \mod p.$$

若 $x=\frac{p-1}{2}$ 是一合数，则此关系式并无多大意思，因为我们已经知道如何利用普通代数知识对合数指数情况的 a^x-1 进行因式分解. 但当 x 为素数时，没有代数方法可用，这时上面的关系式如可利用，即能用于分解 a^x-1. 小于 100 的 x 的素数值，使 p 也是上述八种形式之一的素数，只有 41 与 53，与之对应的 p 值是 83 与 107.

故知 $10^{41}-1$ 能被 83 整除，$10^{53}-1$ 能被 107 整除. 在探索重一数的除数时尚有一些定理可用，但从总体看来，在我们的知识方面还存在着很大的黑洞，正如表 41 所显示的那样.

尽管表 41 只考虑素数指数，但把 10^y-1 的全部素因子统统找出来，即便指数是个合数，仍然决非易事. 甚至对如此小的上限 100 来说，低于此上限的一切 y 值，也还有大量工作要做. 设 y 是 3 的某个偶数倍数，譬如说 48，让我们试行分解一下它所对应的数字. 显然 $10^{48}-1$ 是平方差，故可分解成 $(10^{24}+1)(10^{24}-1)$. 第一个因子是两个立方数之和，故可分解为 $(10^8+1)(10^{16}-10^8+1)$；第二个因子仍是平方差，因而可以继续分解. 但像 $10^{16}-10^8+1$ 这样的表达式简直啃不动，很难分解. "代数"上看来，这是个素因子，没有什么一般方法可使它分解为两个次数较低的实因子. 特殊情况下，这种表达式可能会有因子，但是 $10^{16}-10^8+1=9\ 999\ 999\ 900\ 000\ 001$ 则是一个素数. 要判定这一点并非易事，直到最近才把它弄清楚. 下面的奇怪表格似乎表明在很小范围内此类数字呈现某种规律性，然后却完全乱套了. 这种现象在数论领域里司空见惯，匆促加以推广

有多么危险！

x	$(a^{2x}-a^x+1)$	数值	性质
1	10^2-10+1	91	合数
2	10^4-10^2+1	9901	素数
3	10^6-10^3+1	999001	合数
4	10^8-10^4+1	99990001	素数
5	$10^{10}-10^5+1$	9999900001	合数
6	$10^{12}-10^6+1$	999999000001	素数
7	$10^{14}-10^7+1$	99999990000001	合数
8	$10^{16}-10^8+1$	9999999900000001	素数
9	$10^{18}-10^9+1$	999999999000000001	合数
10	$10^{20}-10^{10}+1$	99999999990000000001	合数（多么遗憾！）

[85]

表 42　$(a^{2x}-a^x+1)$的数值因子，在代数上它是 $(a^{3x}+1)/(a^x+1)$的素因子(既约代数式)

如果我们想完成 $10^{48}-1$ 的分解，就要把 $10^{24}-1$ 继续进行因子分解：

$$10^{24}-1=(10^{12}+1)(10^6+1)(10^3+1)(10^3-1)$$
$$=(10^4+1)(10^8-10^4+1)(10^2+1)(10^4-10^2+1)$$
$$\times(10+1)(10^2-10+1)(10-1)(10^2+10+1).$$

上表已明确告诉我们，第二与第四个因子得出素数. 第一因子 $10^4+1=10001$ 数值很小，在因子表中可以查到它等于 $73\cdot137$. 因子 $10^2+1=101$ 是个素数；$10+1=11$ 也是素数；

$$10^2-10+1=91=7\cdot13;\quad 10-1=9=3^2;$$

而

$$10^2+10+1=111=3\cdot37.$$

因子 10^8+1 可被 17 整除，而其商 5882353 是个素数，于是 $10^{48}-1$ 的最终素因子分解为：

$$17\cdot5882353\cdot9999999900000001\cdot73\cdot137$$

$\cdot 99990001 \cdot 101 \cdot 9901 \cdot 11 \cdot 7 \cdot 13 \cdot 3^3 \cdot 37.$

由此可见，把数码1重复48的数，亦即$(10^{48}-1)/9$，基本上就是以上分解结果，只需用3来替代3^3，以照应分母上的9.

表41中非常简练的话"素数"或"合数"对于诸如$(10^{23}-1)/9$这样的"重一数"所提供的信息未免过于贫乏了.M·克莱契克在其专著《数论研究》的第二卷里曾专门花费一章篇幅，详细描述了他用一番心血以证明该数确实是一个素数.此事的工作量十分庞大，其中也不无幽默情趣，因为他的结论与雷默博士(见第3章)的结论显然并不一致.野心勃勃的读者们，你们不要急急忙忙地去探讨$(10^{47}-1)/9$，最好还是先去参考一下克莱契克的著作.

10的高次方并非只是单纯的数学游戏.虽然这同我们此处的讨论有点文不对题，还是值得提一下，在长距离传输线上，电话交谈大致被放大了10^{4000}倍.哥伦比亚大学教授爱德华·卡斯纳(Edward Kasner)曾有过异想天开的说法，他把10^{100}叫做一个"戈戈尔"(googol)，而把$10^{10^{100}}$叫做一个"戈戈普列克斯"(googolplex).因此40000分贝(4000贝)的电话交谈衰减受到 [86] 了超过$(\text{googol})^{40}$的放大.这种超天文数字到底是什么样子？我们不妨作个比较：150亿光年(美国加利福尼亚州大橡树地区的射电望远镜所能观测到的最大距离)与小小的原子核半径之比也不过是10^{39}而已.

参考文献

Bickmore, C. E. "On the Numerical Factors of a^n-1," *Messenger of Mathematics*, **25**(1895), 1.

Dickson, L. E. *History of the Theory of Numbers*. 3 vols. New York: Chelsea Publishing Co., 1950.

Green, E. I. "The Evolving Technology of Communication,"

Electrical Engineering, **78**(1959), 473.

Kasner, E., and Newman, J. *Mathematics and the Imagination*. New York: Simon and Schuster, 1940.

Kraitchik, M. *Recherches sur la Théorie des Nombres*, *Vols. I, II*. Paris: Gauthier-Villars et Cie., 1924, 1929.

Lehmer, D. H. "Test for Primality by the Converse of Fermat's Theorem," *Bulletin of the American Mathematical Society*, **33**(1927), 327.

——. "A Further Note on the Converse of Fermat's Theorem," *Bulletin of the American Mathematical Society*, **34** (1928), 54.

——. "On the Number $(10^{23}-1)/9$," *Bulletin of the American Mathematical Society*, **35**(1929), 349.

Reid, L. W. *Elements of the Theory of Algebraic Numbers*. Baltimore: Johns Hopkins Press, 1946.

Shanks, W. "On the Number of Figures in the Period of the Reciprocal of Every Prime Number Below 20000," *Proceedings of the Royal Society of London*, **22**(1873), 200.

——. "Given the Number of Figures (Not Exceeding 100) in the Reciprocal of a Prime Number, to Determine the Prime Itself," *Proceedings of the Royal Society of London*, **22** (1873), 381.

——. "On the Number of Figures in the Reciprocal of Every Prime Between 20000 and 30000," *Proceedings of the Royal Society of London*, **22**(1873), 384.

[87]

第12章 欧拉函数

在与欧拉的ϕ函数打交道时，某些看来似乎平铺直叙的问题会对粗心大意者形成许多陷阱. 该函数是小于一个给定整数并与之互质的整数个数. 如果人们要把一个相对说起来较小的数目，例如 72，表为“素数幂的连乘积”，一般不会碰到什么特殊困难. 我们把该数分解，就像是一个化合物被分解成它的组成元素那样. 素数就是算术里头的元素. 多次用 2 与 3 去除 72，最后得到 $72 = 2^3 \cdot 3^2$. 类似地 $120 = 2^3 \cdot 3 \cdot 5$；而明显看得出其中含有 2，3，5 因子的 60840，最终可以分解成 $2^3 \cdot 3^2 \cdot 5 \cdot 13^2$. 我们已注意到，任意正整数 N 分解为素数幂连乘积的一般表达式是

$$N = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_n^{a_n}. \qquad \text{(公式 A)}$$

在教科书中已证明，小于 N 并与之互质(除 1 之外无其他公因子)的整数个数可由下式给出：

$$\phi(N) = p_1^{a_1-1}(p_1 - 1)p_2^{(a_2-1)}(p_2 - 1) \cdot p_3^{a_3-1}(p_3 - 1) \cdots p_n^{a_n-1}(a_n - 1). \qquad \text{(公式 B)}$$

此函数可记为 $\phi(N)$，读作“N 的 ϕ”，ϕ 是一个希腊字母，发音为 fee. 例如：

$$\phi(72) = \phi(2^3 \cdot 3^2) = 2^2(2 - 1) \cdot 3^1(3 - 1) = 4 \cdot 1 \cdot 3 \cdot 2 = 24,$$

$$\phi(120) = \phi(2^3 \cdot 3 \cdot 5) = 2^2(2-1) \cdot 3^0(3-1) \cdot 5^0(5-1)$$
$$= 4 \cdot 1 \cdot 1 \cdot 2 \cdot 1 \cdot 4 = 32.$$

$$\phi(60840) = \phi(2^3 \cdot 3^2 \cdot 5 \cdot 13^2)$$
$$= 2^2(2-1) \cdot 3^1(3-1) \cdot 5^0(5-1) \cdot 13^1(13-1)$$
$$= 4 \cdot 1 \cdot 3 \cdot 2 \cdot 1 \cdot 4 \cdot 13 \cdot 12 = 14976.$$

值得注意的是当一素数在公式 A 仅出现一次方时，由于 $p^0=1$，从而它在公式 B 中不再出现[1]．正是由于这种“缺席”，再加上其他许多原因，许多趣题即随欧拉 ϕ 函数而来．[88]

Ⅰ．对某个给定数，用公式 B 来表达 $b=\phi(N)$，究竟有多少种方法？要求把它全部求出来，并为之提供一种实际可操作的办法．

Ⅱ．从这些 $\phi(N)$ 值求出一切 N．

Ⅲ．找出不能纳入这一表达形式的数 b．

解决这些问题时甚至不一定要知道 $\phi(N)$ 的意义：小于 N 且与之互质的整数个数．纯然从形式上看问题，公式 A 定义了一个数 N，而公式 B 只是 N 的一个函数．只要根据这两个公式即可解决问题．但对一给定数 b 求出所有的 N，还是需要一些机智，并在实践时找到一些具体操作规则．

在第Ⅰ类问题中，若 $b=6$，则 $3^1(3-1)$ 肯定是一种通过公式 B 来表达它的办法．若 $b=8$，则有一解是 $2^3(2-1)$．但是，尽管我们试而又试，$b=14$ 却无法作出这种表达．粗粗一瞥之下，$b=10$ 好像也是这样，可是 $11^0(11-1)$ 却能满足要求．现在请你们再找出一解来．† 然后，还要找出用此形式来表达 2 的三种方法．†

若 $N=1$，则由公式 B，

$$\phi(1) = 1^{1-1}(1-1) = 1^0 \cdot 0 = 1 \cdot 0 = 0;$$

[1] 仅指此素数 p 本身，但 $p-1$ 还是要出现的．故此说法有语病．——译者注．

但是,1 是被认为与任何正整数互质的,也包括它自己,所以 $\phi(1)=1$,而不受公式 B 的制约.

由公式 B 来表达一个整数 b,意味着相应地可由公式 A 来表达 N,因此满足 $\phi(N)=b$ 的 N 的个数与通过公式 B 来表达 b 的方法数是一样的.(上文已提出过作为例外的 1;$\phi(2)$ 与 $\phi(1)$ 都等于 1,但对 $b=1$,只能写出一种表达法,即 $2^0(2-1)$,所以 $\phi(1)=1$是由定义规定,而不是由公式给出的.)这就引发了一个诱人的问题:是否存在着一个正整数 N,它的 $\phi(N)=b$ 是唯一的,或者说,对某个 $b=\phi(N)$而言,只存在一个解答 N? 现已证明,对一切小于 10^{400}的正整数,这种 N 是不存在的.看来此种 N 的存在极不可能.(地球上所有的水滴数小于 10^{30}.)在此上限以下,对一给定的 $b=\phi(N)$,至少可以找到 N 的两个解答.这就是说,如果一个奇数 N 为一解,则 $2N$ 亦必为解;若偶数 $N=2(2x+1)$是一解,则奇数 $2x+1$ 也必是解.由此可推出,若存在一个 [89] 数 N,而它的 $\phi(N)$是唯一的话,则 N 必定是 4 的倍数.

容易证明,b 不能为奇数,除掉唯一的例外 $b=1$ 之外,此时它有解 $2^0(2-1)$.公式 B 表明,至少要有一个 b 的因子(p_1-1),而对一切大于 2 的素数而言,当然它必是偶数.若 $p_1=2$,则 $p_1^{a_1-1}$ 是偶数,在 $a_1=1$ 时,那就是上文已提到过的唯一例外.

用公式 B 来表达 6 时,$3^1(3-1)$只是四种方法之一.其他三种办法如下:

$$7^0(7-1) = 6,$$
$$2^0(2-1)\cdot 7^0(7-1) = 6,$$
$$2^0(2-1)\cdot 3^1(3-1) = 6.$$

只须把相应的 N 求出来,我们即可看出它们是不同解,详见附表 43.

也可以反其道而行之,如照公式 A,先有 9,7,14,18,再用公式 B 来算 $\phi(N)$,则可验证每种情况的结果都是 6.表 43 中顺

便也给出了小于 N 并与之互质的各数.

N	小于 N 并与之互质的正整数	$b=\phi(N)$ 按公式 B 的表达法
$7^1=7$	1;2;3;4;5;6	$7^0(7-1)=6$
$3^2=9$	1;2;4;5;7;8	$3^1(3-1)=6$
$2\cdot7=14$	1;3;5;9;11;13	$2^0(2-1)\cdot7^0(7-1)=6$
$2\cdot3^2=18$	1;5;7;11;13;17	$2^0(2-1)\cdot3^1(3-1)=6$

表 43　$\phi(N)=6$ 时的 N 值

在 $N=14$ 与 18 时可看到,肤浅的平凡解 $2^0(2-1)=1$ 一旦与其他数字配合即可得出不同的解答.

对 $\phi(N)=12$,存在着六解,它们是:

$$13^0(13-1);2^0(2-1)\cdot13^0(13-1);3^0(3-1)\cdot7^0(7-1);$$
$$2^0(2-1)\cdot3^0(3-1)\cdot7^0(7-1);2^1(2-1)\cdot3^1(3-1);$$
$$2^1(2-1)\cdot7^0(7-1).$$

对应的 N 值是 13,26,21,42,36,28. 它们中的每一个都恰恰含有 12 个整数(包括 1 在内),这些整数小于 N 本身,除 1 之外与[90]它也无公因子.

解决第Ⅱ类问题要小心;基本事实被逮住以前经常会漏过我们的眼睛. 前已说过,像 $b=14=2\cdot7$ 这样的数目不能纳入 $p_1^{a_1}(p_1-1)$这种形式,重复几次的乘积也不行. 表 44 中另外给出了一些不可能值.

14	62	90	122	152
26	68	94	124	154
34	74	98	134	158
38	76	114	142	170
50	86	118	146	174

表 44　$\phi(N)$的不可能值

如果给定的数 b 具有性质:(1)一个素数幂的二倍:$2p^a$,(2) p 大于 3,(3)$2p^a+1$ 是合数,则 b 不能纳入公式 B. 但这不过是许多种不可能情况之一. 我们把这些情况的一部分留给读者去

思考.†

像解决Ⅰ、Ⅱ类问题那样，搞出一些坚不可摧的规则是极有兴趣的，但颇伤脑筋.当读者完成这件工作之后，也许他会愿意解决下面五个问题：给出 $b=\phi(N)$，求 N，此处的 b 值为 1；72；144；480；以及 $6600=2^3\cdot 3\cdot 5^2\cdot 11$.†

卡米凯尔(R. D. Carmichael)曾对从 1 到 1000 的给定 b 值，表列出 $\phi(N)=b$ 的一切 N 值.正如人们所预料，这要花费很多精力；例如，满足 $\phi(N)=960$ 的 N 值就有 47 个.当 b 不超过 50 时，解数最多的情况是 $b=48$，它有 11 个解.在 50 以下，只有 21 个 b 值才可能有解，因而当 b 不超过这个限度时，编制满足条件的解答的表格所要花费的工作量还不算太大，也许读者们愿意试一试.†

*　　*　　*

小于给定数 N 并与之互质的整数，当然是素数或合数均有可能.但在某些情况下，它们竟然全是素数，例如，当 $N=2,3,4,6,8,12,18,24,30$.例如 $\phi(18)=6$，小于 18 且与之互质的数为 1,5,7,11,13,17.这个关系是非常奇妙的，因为只有这九个数值才能有如此现象；大于 30 的任何整数都没有这一性质. [91]

*　　*　　*

欧拉 ϕ 函数有许多引人注目的现象，有些现象非常复杂.其中一个颇为令人惊奇的现象是：小于 n 并与之互质的各正整数之和等于 $\left(\frac{n}{2}\right)[\phi(n)]$，此处要假定 n 大于 1.为了证明这一点，应注意到：若 I 是一个与 n 互质的整数，则 $n-I$ 亦必然如此.这两数之和是 n.但这些整数有 $\frac{\phi[N]}{2}$ 对，因此，各对整数之和必为 $n\left[\frac{\phi(N)}{2}\right]$，亦即 $(n/2)[\phi(N)]$.

*　　*　　*

方程 $k\cdot\phi(x)=x+1$ 与 $k\cdot\phi(x)=x-1$ 是有趣的.先考虑

前者，当 $k=1$，将有 $\phi(x)=x+1$，由于 $\phi(x)$ 决不能大于 x，所以这根本不可能成立. 当 $k=2$，将有 $2\cdot\phi(x)=x+1$，它有一解 $x=3$，另外的解见附表 15. 当 $k=3$，有一个解 $x=2$，但如果有另外的解时，则它至少是 32 个不同素数的乘积！

k	x	$x+1$	$\phi(x)$
1	无解	…	…
2	3	2^2	2^1
2	$3\cdot 5$	2^4	2^3
2	$3\cdot 5\cdot 17$	2^8	2^7
2	$3\cdot 5\cdot 17\cdot 257$	2^{16}	2^{15}
2	$3\cdot 5\cdot 17\cdot 353\cdot 929$	$2^{18}\cdot 11\cdot 29$	$2^{17}\cdot 11\cdot 29$
2	$3\cdot 5\cdot 17\cdot 257\cdot 65537$	2^{32}	2^{31}
2	$3\cdot 5\cdot 17\cdot 353\cdot 929\cdot 83623937$	$2^{36}\cdot 11^2\cdot 29^2$	$2^{35}\cdot 11^2\cdot 29^2$
2	至少 7 个不同素数之积	—	—
3	2	3	1
3	至少 32 个不同素数之积	—	—

表 45　$k\cdot\phi(x)=x+1$ 的解

现在考虑 $k\cdot\phi(x)=x-1$. 当 $k=1$，则任何素数 x 都是方程的解，因为此时的 $\phi(x)$ 必然等于 $x-1$. 公式 B 已清楚地表明当 x 为合数时，$\phi(x)$ 与 x 的差别必定大于 1，因此，决不可能有任何合数满足方程 $1\cdot\phi(x)=x-1$.〔92〕

当 k 大于 1 时，x 肯定是合数，因对素数来说，$\phi(x)$ 正好等于 $x-1$. 但若 x 是合数，则它至少是 7 个不同素数之积. 然而，具体的解答尚未求出. 有人怀疑，对合数 x 而言，解并不存在. 然而要证明这一点难度很大，并不稍逊于证明不存在奇完全数.

当 $k=3$，满足条件的 x 至少是 32 个不同素数因子的乘积. 以上这些事实简要地总结于附表 46 中.

k	x	$x-1$	$\phi(x)$
1	任意素数	$x-1$	$x-1$
2	至少应是 7 个素数的乘积；尚未找到其解答	—	—
3	至少应是 32 个素数的乘积；尚未找到其解答	—	—

表 46　$k\cdot\phi(x)=x-1$ 的解

参考文献

Carmichael, R. D. *Theory of Numbers and Diophantine Analysis*. New York: Dover Publications, Inc., 1959.

——. "Notes on the Simplex Theory of Numbers," *Bulletin of the American Mathematical Society*, **15** (1908—1909), 217.

——. "A Table of Values of m Corresponding to Given Values of $\phi(m)$," *American Journal of Mathematics*, **30** (1908), 394.

——. "Note on Euler's ϕ Function," *Bulletin of the American Mathematical Society*, **28**(1922), 109.

Dickson, L. E. *History of the Theory of Numbers*. 3 vols. New York: Chelsea Publishing Co., 1950.

Klee, V. L. "On a Conjecture of Carmichael," *Bulletin of the American Mathematical Society*, **54**(1948), 53.

Lehmer, D. H. "On Euler's Totient Function," *Bulletin of the American Mathematical Society*, **38**(1932), 745. [93]

第13章 古怪的对数——回复原始

这是一个真正的激动.原来人们发现一贯被认为专属连续领域的对数居然在离散领域的数论中有着对等物.在 $10^2=100$ 中,2 是 100 的对数,在 $10^3=1000$ 中,3 是 1000 的对数.对同样的"底数"10,某些中间数的对数,譬如说 500 的对数位于 2 与 3 之间,准确到五位小数,其值为 2.69897.粗看上去,很难想象这种小数近似值会有什么整数对等物.但是,对给定模数而言,任意整数都可准确地表示为某个合适的整数底的乘幂,任何情况下,其指数或"对数"都是整数.研究这种对数很有趣,在数论里头,它们称为"指数"(Indices).①

取定模 13,再任选一个底,例如 2,让我们来看一看,一切整数是怎样表示为 2 的乘幂的.此时有 $2^{12}\equiv1$, $2^1\equiv2$, $2^4\equiv3$, $2^2\equiv4$, $2^9\equiv5$, $2^5\equiv6$, $2^{11}\equiv7$, $2^3\equiv8$, $2^8\equiv9$, $2^{10}\equiv10$, $2^7\equiv11$, $2^6\equiv12$.概括得很完全.数与指数都没有重复,它们之间存在着一一对应.是否总是如此呢?让我们再用 3 来作底数试试.这时将有 $3^1\equiv3$, $3^2\equiv9$, $3^3\equiv1$, $3^4\equiv3$, $3^5\equiv9$, $3^6\equiv1$, $3^7\equiv3$, $3^8\equiv9$, $3^9\equiv1$, $3^{10}\equiv3$, $3^{11}\equiv9$, $3^{12}\equiv1$.由此可见,虽然指数范围是从 1 到 12,可是整数(剩余)却老是 1,3,9.对于一个给定的模数,要想得到一个"完全剩余系",只能选用某些特定的底数才行;它们必须是模的任

① 为了与通常的指数表示区别,也有译成"指标"的.今据《中国大百科全书·数学卷》,仍称指数.——译者注.

意一个原根. 让我们重新回忆一下原根的概念,所谓素数模 p 的原根 g,是指使同余式 $g^e \equiv 1 \bmod p$ 得以成立的最小指数 e 必须为 $p-1$. 整数 13 只有四个原根:2,6,7,11,它们中每个数的乘幂都能形成完全剩余系,如附表 47 所示. 在有关指数的问题中,表中四列中的任一列都可使用. 正如对数问题中,常用对数的底10与自然对数的底e都可应用一样. 然而,对数问题中任何其他底数都可使用,然而在这里的指数问题中却只能使用 13 的四个原根之一. [94]

数 (剩余)	A列 原根 2	B列 原根 6	C列 原根 7	D列 原根 11
1	12(或 0)	12(或 0)	12(或 0)	12(或 0)
2	1	5	11	7
3	4	8	8	4
4	2	10	10	2
5	9	9	3	3
6	5	1	7	11
7	11	7	1	5
8	3	3	9	9
9	8	4	4	8
10	10	2	2	10
11	7	11	5	1
12	6	6	6	6

表 47 指数表,模 13

用对数做乘法,我们需将所乘各数之对数相加. 类似步骤对于指数也行. 就素数模 p 而言,任何数的最大指数是 $p-1$;因而在乘法问题中,若结果超过 $p-1$,则可去掉 $p-1$ 的整数倍而结果不受影响.

我们将用对数与指数分别求解两个问题来作有趣对比,前者选用常用对数的底 10,而后者选用模 13 的原根 11.

求解 $6\cdot8\cdot9=x$	求解 $6\cdot8\cdot9=x \bmod 13$
$\log_{10}6=0.77815$	$\text{ind}_{11}6=11$
$\log_{10}8=0.90309$	$\text{ind}_{11}8=9$
$\log_{10}9=0.95424$	$\text{ind}_{11}9=8$
相加，$\log_{10}x=2.63548$	相加，$\text{ind}_{11}x=28\equiv4 \bmod 12$
$x=432$	$x\equiv3 \bmod 13$

对数问题几乎无需解释，我们只要查一下 2.63548 的反对 [95] 数即可得出 x. 在同余式问题中，x 的指数是 28，即 $x\equiv 11^{28} \bmod 13$，但由于 $11^{12}\equiv1 \bmod 13$（由费马小定理），所以我们可在指数中去掉 12 的整数倍，因为这一步相当于用 1 去除，故而结果不变. 于是得出 $x\equiv11^4 \bmod 13$，现在我们在附表的 D 列中进行逆操作，就像查找 2.63548 的反对数那样，便可看到与指数 4 对应的是剩余 3，故有 $6\cdot8\cdot9\equiv3 \bmod 13$.

讲对数时，我们可用换底公式，把底 a 转为底 b：

$$\log_b N=\log_a N\cdot\log_b a.$$

类似地有：

$$\text{ind}_b N\equiv\text{ind}_a N\cdot\text{ind}_b\, a \mod (p-1).$$

由此公式，我们可以从表 47 B 列的指数得出该表 A 列的指数：

$$\text{ind}_2 N\equiv\text{ind}_6 N\cdot\text{ind}_2 6\equiv(\text{ind}_6 N)\cdot5 \mod 12.$$

即表中以 2 为底的指数可从以 6 为底的指数得出，只须乘 5 再取同余就行. 由此便得 60，25，40，50，45，5，35，15，20，10，55，30，按模 12 同余于 12（或 0），1，4，2，9，5，11，3，8，10，7，6. 而这些数便是表中 A 列的指数.

利用指数表，我们可以解决诸如 $4\cdot5^x\equiv9 \bmod 13$ 一类的乘幂同余问题，犹如我们利用对数去解指数方程. 让我们任取一

个底 2，求出相应的指数，于是有 $\mathrm{ind}_2 4 + x \cdot \mathrm{ind}_2 5 \equiv \mathrm{ind}_2 9 \pmod{12}$. 由于 $\mathrm{ind}_2 5 = 9$，代入后得 $9x \equiv \mathrm{ind}_2 9 - \mathrm{ind}_2 4 \equiv 8 - 2 \equiv 6 \pmod{12}$. 从而 $3x \equiv 2 \pmod 4$（将上面同余式的两边及模都用 3 除）. 最后得 $x \equiv 2 \pmod 4$，于是 $4 \cdot 5^2 = 100$ 按模 13 同余于 9，而 2 是使此式成立的 x 的最小值. x 的其他可用之值为 $x = 6$，10，14，…，$(4K+2)$.

许多类型的其他问题也可通过指数求解.

*　　　*　　　*

19 世纪初叶辉耀天际的一位数学明星雅可比（C. G. J. Jacobi）曾对 1000 以下的所有素数编出了剩余与指数表，并以《算术宝典》的名称公开发行. 艾伦·克宁汉在其著作《主指数，剩余指数，原根与标准同余式》中列出了 25409 以下一切素数的最小正原根与最小负原根. 给出 b 与 p 后，能使 $b^e \equiv 1 \bmod p$ 成立的最小指数 e 称为"按模 p，b 所属的指数"，或者简单地说成"b 的主指数，模 p". $p-1$ 被主指数除得之商叫做"剩余指标". 例如，在 $9^e \equiv 1 \pmod{13}$ 中，3 是最小的指数，故而 3 便是主指数，而 9 的剩余指标（模 13）为 4. [96]

如能知道各种底数在不同模数下的主指数与剩余指标，那将是便利而有用的. 在这一研究方向，应该提到上述克宁汉的著作. 在该书中他列出了 25409 以下的一切素数模，以及与底 2，3，5，6，7，10，11，12 相应的剩余指标与主指数. 向克斯对底数 10 与 120000 以下的一切素数模也做了与此类似的工作，这在第 10 章中已经讲过.

作为一种消遣，本书作者对 100 以下的一切素数模及其乘幂，编出了整数 1 到 100 的主指数表，这些数据参见附表 48. 例如，在 13 开头的那一列中，我们可以查到从 1 开始、迄于 100 的连续正整数的主指数. 譬如说，对整数 9 而言，该项指数为 3；对 6 与 7，指数为 12，因此 6 与 7 是 13 的原根. 对大于 12 的底数 a，则可按模 13 取同余，例如

$$9^3 \equiv 22^3 \equiv 35^3 \equiv 1 \mod 13.$$

表中，与模数不互质的底数需留出空白，表中以“—”号表记，其时余数不可能为1.

由表48可得到从3至97共24个素数的最小原根.它们另列于表49中.值得注意的是2作为原根出现得甚为频繁——竟达12次之多.

由表48易于得出，对任意给定的底数a，使费马定理得以成立的合数模.例如，设人们需求出满足同余式$17^{x-1} \equiv 1 \mod x$的合数x.沿着$a=17$的横行看过去，然后找出表中两数，其最小公倍数除两数所属列之首数乘积时余数为1.例如沿[97]着$a=17$看过去，可以找到4与2所属两列之首数为5与3^2，此时，4与2的最小公倍数为4，用4去除$5 \cdot 3^2=45$时余数为1，从而得出$17^4 \equiv 1 \mod 45$.于是得出所需之关系式$17^{44} \equiv 1 \mod 45$.

此法则之成立理由不难理解.对给定的a与p，该表已给出使$a^e \equiv 1 \mod p$成立的最小指数e.如果对选定的“a”，我们已找出$a^{e_1} \equiv 1 \mod p_1$以及$a^{e_2} \equiv 1 \mod p_2$，则$e_1$，$e_2$的最小公倍数$e$可用作每个同余式中的指数，即$a^e \equiv 1 \mod p_1$与$a^e \equiv 1 \mod p_2$.由于$p_1$，$p_2$互质，故同余式对模$p_1p_2$也成立，于是有$a^e \equiv 1 \mod p_1p_2$.如果指数改为$e$的整数倍$ke$，同余式当然也成立.若用$e$去除$p_1p_2$而留下余数1，那意味着$p_1p_2-1$必能被$e$整除，即$p_1p_2-1=ke$.从而我们最后得出$a^{ke}=a^{p_1p_2-1} \equiv 1 \mod p_1p_2$，这就是我们所要证明的.

应注意合数模所含的素因子可能不止两个.例如，对$a=41$，我们可以选取2，1，2，其所属列之首数为素数3，5，7.而2，1，2的最小公倍数是2，用它去除$3 \cdot 5 \cdot 7=105$时余数为1，于是可得出$41^2 \equiv 1 \mod 105$，以及$41^{104} \equiv 1 \mod 105$.

a	2	3	2^2	5	7	2^3	3^2	11	13	2^4	17	19	23	5^2	3^3	29	31	2^5	37	41	43	47	7^2	53	59	61	2^6	67	71	73	79	3^4	83	89	97	a
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	—	2	—	4	3	—	6	10	12	—	8	18	11	20	18	28	5	—	36	20	14	23	21	52	58	60	—	66	35	9	39	54	82	11	48	2
3	1	—	2	4	6	2	—	5	3	4	16	18	11	20	—	28	30	8	18	8	42	23	42	52	29	10	16	22	35	12	78	—	41	88	48	3
4	—	1	—	2	3	—	3	5	6	—	4	9	11	10	9	14	5	—	18	10	7	23	21	26	29	30	—	33	35	9	39	27	41	11	24	4
5	1	2	1	—	6	2	6	5	4	4	16	9	22	—	18	14	3	8	36	20	42	46	42	52	29	30	16	22	5	72	39	54	82	44	96	5
6	—	—	—	1	2	—	—	10	12	—	16	9	11	5	—	14	6	—	4	40	3	23	14	26	58	60	—	33	35	36	78	—	82	88	12	6
7	1	1	2	4	—	2	3	10	12	2	16	3	22	4	9	7	15	4	9	40	6	23	—	26	29	60	8	66	70	24	78	27	41	88	96	7
8	—	2	—	4	1	—	2	10	4	—	8	6	11	20	6	28	5	—	12	20	14	23	7	52	58	20	—	22	35	3	13	18	82	11	16	8
9	1	—	1	2	3	1	—	5	3	2	8	9	11	10	—	14	15	4	9	4	21	23	21	26	29	5	8	11	35	6	39	—	41	44	24	9
10	—	1	—	—	6	—	1	2	6	—	16	18	22	—	3	28	15	—	3	5	21	46	42	13	58	60	—	33	35	8	13	9	41	44	96	10
11	1	2	2	1	3	2	6	—	12	4	6	3	22	5	18	28	30	8	6	40	7	46	21	26	58	4	16	66	70	72	39	54	41	22	48	11
12	—	—	—	4	6	—	—	1	2	—	16	6	11	20	—	4	30	—	9	40	42	23	42	52	29	15	—	66	35	36	26	—	41	8	16	12
13	1	1	1	4	2	2	3	10	—	4	4	18	11	20	9	14	30	8	36	40	21	46	14	13	58	3	16	66	70	72	39	27	82	88	96	13
14	—	2	—	2	—	—	6	5	1	—	16	18	22	10	18	28	15	—	12	8	21	23	—	52	58	6	—	11	10	72	26	54	82	88	96	14
15	1	—	2	—	1	2	—	5	12	2	8	18	22	—	—	28	10	2	36	40	21	46	7	13	29	15	4	11	35	72	26	—	82	88	96	15
16	—	1	—	1	3	—	3	5	3	—	2	9	11	5	9	7	5	—	9	5	7	23	21	13	29	15	—	33	35	9	39	27	41	11	12	16
17	1	2	1	4	6	1	2	10	6	1	—	9	22	20	6	4	30	2	36	40	21	23	42	26	29	60	4	33	10	24	26	18	41	44	96	17
18	—	—	—	4	3	—	—	10	4	—	1	2	11	4	—	28	15	—	36	5	42	23	3	52	58	60	—	66	35	18	13	—	82	44	16	18
19	1	1	2	2	6	2	1	10	12	4	8	—	22	10	3	28	15	8	36	40	42	46	6	52	29	30	16	33	35	36	39	9	82	88	32	19
20	—	2	—	—	2	—	6	5	12	—	16	1	22	—	18	7	15	—	36	20	42	46	14	52	29	5	—	66	7	72	39	54	82	44	32	20
21	1	—	1	1	—	2	—	2	4	4	4	18	22	5	—	28	30	8	18	20	7	23	—	52	29	12	16	33	70	24	13	—	41	44	96	21
22	—	1	—	4	1	—	3	—	3	—	16	18	2	20	9	14	30	—	36	40	14	46	7	52	29	15	—	11	70	8	13	27	82	22	4	22
23	1	2	2	4	3	2	6	1	6	2	16	9	—	20	18	7	10	4	12	10	21	46	21	4	58	20	8	33	14	36	3	54	41	88	96	23
24	—	—	—	2	6	—	—	10	12	—	16	9	1	2	—	7	30	—	36	40	21	23	42	13	58	20	—	11	35	12	6	—	82	88	24	24
25	1	1	1	—	3	1	3	5	2	2	8	9	11	—	9	7	3	4	18	10	21	23	21	26	29	15	8	11	5	36	39	27	41	22	48	25

表 48 a 所属的指数，模 p 与模 p^e

a	2	3	2^2	5	7	2^3	3^2	11	13	2^4	17	19	23	5^2	3^3	29	31	2^5	37	41	43	47	7^2	53	59	61	2^6	67	71	73	79	3^4	83	89	97	a
26	—	2	—	1	6	—	2	5	—	—	8	3	11	1	2	28	6	—	3	40	42	46	42	52	29	60	—	33	14	72	39	6	41	88	96	26
27	1	—	2	4	2	2	—	5	1	4	16	6	11	20	—	28	10	8	6	8	14	23	14	52	29	10	16	22	35	4	26	—	41	88	16	27
28	—	1	—	4	—	—	1	10	12	—	16	9	22	20	1	2	15	—	18	40	42	23	—	13	29	20	—	66	70	72	78	3	41	88	32	28
29	1	2	1	2	1	2	6	10	3	4	16	18	11	10	18	—	10	8	12	40	42	46	7	26	29	12	16	3	35	72	78	54	41	88	96	29
30	—	—	—	—	3	—	—	10	6	—	4	3	22	—	—	1	2	—	18	40	42	46	3	4	58	60	—	6	7	24	78	—	41	88	32	30
31	1	1	2	1	6	2	3	5	4	2	16	6	11	5	9	28	—	2	4	10	21	46	6	52	58	60	2	66	70	72	39	27	41	88	48	31
32	—	2	—	4	3	—	6	2	12	—	8	18	11	4	18	28	1	—	36	4	14	23	21	52	58	12	—	66	7	9	39	54	82	11	48	32
33	1	—	1	4	6	1	—	—	12	1	2	18	22	20	—	14	5	1	9	20	42	46	42	52	58	20	2	33	70	72	26	—	41	88	8	33
34	—	1	—	2	2	—	3	1	4	—	—	18	22	10	9	14	30	—	9	40	42	23	14	52	58	5	—	66	14	72	78	27	82	4	32	34
35	1	2	2	—	—	2	2	10	3	4	1	9	11	—	6	14	5	8	36	40	7	46	—	52	29	60	16	33	70	36	78	18	82	88	3	35
36	—	—	—	1	1	—	—	5	6	—	8	9	11	5	—	7	3	—	2	20	3	23	7	13	29	30	—	33	35	18	39	—	41	44	6	36
37	1	1	1	4	3	2	1	5	12	4	16	2	22	20	3	28	6	8	—	5	6	23	21	26	58	20	16	3	7	9	78	9	41	8	96	37
38	—	2	—	4	6	—	6	5	2	—	4	—	22	20	18	14	15	—	1	8	21	46	42	26	58	20	—	6	35	36	13	54	41	88	96	38
39	1	—	2	2	3	2	—	10	—	2	16	1	11	10	—	28	5	4	36	20	14	46	21	52	58	30	8	33	14	72	78	—	82	11	96	39
40	—	1	—	—	6	—	3	10	1	—	16	18	22	—	9	28	15	—	18	2	21	46	42	26	58	12	—	11	35	72	39	27	41	44	96	40
41	1	2	1	1	2	1	6	10	12	2	16	18	11	5	18	4	15	4	18	—	7	46	14	52	29	10	8	66	14	18	26	54	41	88	96	41
42	—	—	—	4	—	—	—	5	3	—	8	9	22	20	—	14	30	—	36	1	2	23	—	13	58	15	—	22	70	72	39	—	82	44	32	42
43	1	1	2	4	1	2	3	2	6	4	8	9	22	4	9	28	30	8	4	20	—	46	7	26	58	60	16	22	35	24	78	27	82	88	24	43
44	—	2	—	2	3	—	2	—	4	—	16	9	22	10	6	28	30	—	9	8	1	46	21	13	58	60	—	66	70	72	39	18	41	22	48	44
45	1	—	1	—	6	2	—	1	12	4	16	3	2	—	—	7	15	8	12	10	14	46	42	52	29	30	16	22	7	72	39	—	82	11	32	45
46	—	1	—	1	3	—	1	10	12	—	16	6	—	5	3	4	10	—	9	20	42	2	21	13	29	30	—	66	10	4	13	9	82	88	32	46
47	1	2	2	4	6	2	6	5	4	2	4	9	1	20	18	28	5	2	3	40	7	—	42	13	58	3	4	33	70	72	78	54	82	44	8	47
48	—	—	—	4	2	—	—	5	3	—	16	18	11	20	—	28	30	—	6	40	42	1	2	52	29	6	—	66	7	36	78	—	41	88	48	48
49	1	1	1	2	—	1	3	5	6	1	8	3	11	2	9	7	15	2	9	20	3	23	—	13	29	30	4	33	35	12	39	27	41	44	48	49
50	—	2	—	—	1	—	6	10	12	—	2	6	11	—	18	28	15	—	36	4	6	23	1	52	58	4	—	66	35	36	39	54	82	22	8	50
51	1	—	2	1	3	2	—	10	2	4	—	18	22	1	—	14	15	8	12	5	14	23	21	52	29	60	16	66	14	8	39	—	41	88	32	51

表 48 a 所属的指数，模 p 与模 p^α（续）

a	2	3	2^2	5	7	2^3	3^2	11	13	2^4	17	19	23	5^2	3^3	29	31	2^5	37	41	43	47	7^2	53	59	61	2^6	67	71	73	79	3^4	83	89	97	a
52	—	1	—	4	6	—	3	10	—	—	1	18	11	20	9	7	30	—	36	40	21	46	42	2	58	10	—	22	70	24	13	27	82	8	32	52
53	1	2	1	4	3	2	2	5	1	4	8	18	22	20	2	7	30	8	9	40	21	23	4	—	29	20	16	22	70	72	78	6	82	44	48	53
54	—	—	—	2	6	—	—	2	12	—	16	9	11	10	—	7	10	—	36	40	7	23	42	1	58	60	—	33	5	36	78	—	82	88	24	54
55	1	1	2	—	2	2	1	—	3	2	4	9	11	—	1	28	30	4	36	8	42	23	14	52	58	60	8	33	70	9	3	3	82	4	32	55
56	—	2	—	1	—	—	6	1	6	—	16	2	22	5	18	28	3	—	36	40	21	23	—	52	58	15	—	33	70	24	6	54	82	88	96	56
57	1	—	1	4	1	1	—	10	4	2	16	—	22	4	—	2	6	4	36	5	21	46	7	26	29	15	8	66	5	18	26	[illegible]	82	22	96	57
58	—	1	—	4	3	—	3	5	12	—	16	1	11	20	9	—	10	—	18	40	21	46	21	52	2	5	—	22	35	72	26	27	82	88	96	58
59	1	2	2	2	6	2	6	5	12	4	8	18	11	10	18	1	15	8	36	5	7	23	42	26	—	60	16	11	70	72	78	54	41	88	96	59
60	—	—	—	—	3	—	—	5	4	—	8	18	22	—	—	28	10	—	12	40	21	46	21	26	1	2	—	33	35	72	78	—	82	88	96	60
61	1	1	1	1	6	2	3	10	3	4	16	9	22	5	9	28	2	8	36	20	42	23	42	52	58	—	16	66	70	36	26	27	41	88	3	61
62	—	2	—	4	2	—	2	10	6	—	16	9	11	20	6	14	—	—	18	20	42	46	14	26	29	1	—	11	70	72	13	18	82	88	6	62
63	1	—	2	4	—	2	—	10	12	2	16	9	22	20	—	14	1	2	3	40	42	23	—	13	29	60	2	66	70	8	78	—	41	88	32	63
64	—	1	—	2	1	—	1	5	2	—	4	3	11	10	3	14	5	—	6	10	7	23	7	26	29	10	—	11	35	3	13	9	41	11	8	64
65	1	2	1	—	3	1	6	2	—	1	16	6	22	—	18	7	30	1	18	40	14	23	21	52	58	30	1	33	70	6	13	54	41	88	48	65
66	—	—	—	1	6	—	—	—	1	—	8	9	22	5	—	28	5	—	12	10	21	46	42	13	29	30	—	2	10	24	78	—	82	88	48	66
67	1	1	2	4	3	2	3	1	12	4	2	18	22	20	9	14	3	8	18	40	21	46	3	52	58	60	16	—	70	36	13	27	82	11	32	67
68	—	2	—	4	6	—	6	10	3	—	—	3	2	4	18	28	6	—	4	8	21	23	6	13	29	60	—	1	70	72	78	54	41	44	96	68
69	1	—	1	2	2	2	—	5	6	4	1	6	—	10	—	28	15	8	36	40	42	46	14	13	58	20	16	66	70	18	26	—	41	44	32	69
70	—	1	—	—	—	—	3	5	4	—	8	18	1	—	9	4	5	—	9	40	14	46	—	26	58	5	—	22	2	12	78	27	41	88	16	70
71	1	2	2	1	1	2	2	5	12	2	16	18	11	5	6	14	15	4	9	40	42	23	7	52	29	60	8	33	—	18	26	18	82	44	96	71
72	—	—	—	4	3	—	—	10	12	—	4	18	11	20	—	28	15	—	36	10	42	23	21	52	58	4	—	22	1	2	39	—	82	44	48	72
73	1	1	1	4	6	1	1	10	4	2	16	9	11	20	3	28	30	4	2	4	42	46	42	52	58	15	8	33	35	—	39	9	82	22	24	73
74	—	2	—	2	3	—	6	10	3	—	16	9	22	2	18	28	30	—	—	20	21	23	21	52	29	3	—	66	35	1	78	54	82	88	96	74
75	1	—	2	—	6	2	—	5	6	4	16	2	11	—	—	4	30	8	1	40	14	23	42	52	29	6	16	22	35	9	78	—	41	88	4	75
76	—	1	—	1	2	—	3	2	12	—	8	—	22	1	9	28	15	—	36	40	42	46	14	4	29	15	—	11	5	12	39	27	82	88	96	76
77	1	2	1	4	—	2	6	—	2	4	8	1	11	20	18	28	10	8	18	20	42	46	—	13	58	15	16	33	35	9	78	54	41	8	32	77

表 48　a 所属的指数，模 p 与模 p^r（续）

[99]

a	2	3	2^2	5	7	2^3	3^2	11	13	2^4	17	19	23	5^2	3^3	29	31	2^5	37	41	43	47	7^2	53	59	61	2^6	67	71	73	79	3^4	83	89	97	a
78	—	—	—	4	1	—	—	1	—	—	16	18	11	20	—	7	5	—	18	5	7	46	7	26	29	60	—	66	70	72	2	—	41	11	32	78
79	1	1	2	2	3	2	3	10	1	2	16	18	22	10	9	28	30	2	36	8	3	23	3	52	29	60	4	66	35	36	—	27	82	44	16	79
80	—	2	—	—	6	—	2	5	12	—	16	9	22	—	2	14	15	—	4	20	6	46	6	52	29	30	—	66	35	24	1	2	82	44	96	80
81	1	—	1	1	3	1	—	5	3	1	4	9	11	5	—	7	15	2	9	2	21	23	21	13	29	5	4	11	35	3	39	—	41	22	12	81
82	—	1	—	4	6	—	1	5	6	—	16	9	11	4	1	7	15	—	12	—	14	46	42	26	58	12	—	11	70	6	78	1	2	88	96	82
83	1	2	2	4	2	2	6	10	4	4	8	3	22	20	18	7	30	8	9	1	21	23	14	4	58	15	16	33	35	8	39	54	—	88	96	83
84	—	—	—	2	—	—	—	10	12	—	2	6	22	10	—	28	30	—	3	20	7	23	—	52	29	20	—	33	70	72	39	—	1	44	96	84
85	1	1	1	—	1	2	3	10	12	4	—	9	11	—	9	28	10	8	6	8	2	46	7	52	29	20	16	66	10	36	78	27	82	22	16	85
86	—	2	—	1	3	—	6	5	4	—	1	18	22	5	18	2	30	—	9	10	—	46	21	52	29	15	—	33	35	72	78	54	41	88	48	86
87	1	—	2	4	6	2	—	2	3	2	8	3	11	20	—	—	3	4	36	20	1	46	42	52	29	60	8	66	35	72	13	—	41	22	96	87
88	—	1	—	4	3	—	3	—	6	—	16	6	22	20	9	1	6	—	12	40	14	46	21	52	29	10	—	33	10	72	39	27	82	2	24	88
89	1	2	1	2	6	1	2	1	12	2	4	18	22	10	6	28	10	4	36	40	42	23	42	13	58	20	8	11	35	9	13	18	82	—	16	89
90	—	—	—	—	2	—	—	10	2	—	16	18	22	—	—	28	15	—	9	20	7	46	14	26	58	12	—	33	35	24	39	—	41	1	96	90
91	1	1	2	1	—	2	1	5	—	4	16	18	2	5	3	14	10	8	36	4	42	46	—	26	58	60	16	11	7	18	26	9	82	11	12	91
92	—	2	—	4	1	—	6	5	1	—	16	9	—	20	18	14	2	—	36	5	3	46	7	52	58	60	—	11	70	36	39	54	41	88	96	92
93	1	—	1	4	3	2	—	5	12	4	8	9	1	4	—	14	—	8	36	40	6	2	21	26	58	12	16	33	70	72	26	—	41	11	24	93
94	—	1	—	2	6	—	3	10	3	—	8	2	11	10	9	7	1	—	36	40	14	—	42	52	29	20	—	22	14	24	26	27	41	44	48	94
95	1	2	2	—	3	2	6	10	6	2	16	—	11	—	18	28	5	2	18	40	21	1	21	13	29	20	2	66	35	8	39	54	41	88	48	95
96	—	—	—	1	6	—	—	10	4	—	16	1	11	5	—	14	30	—	36	8	21	23	42	26	58	60	—	3	5	36	26	—	82	88	2	96
97	1	1	1	4	2	1	3	5	12	1	16	18	22	20	9	28	5	1	12	40	7	23	2	13	58	30	2	6	14	12	13	27	82	11	—	97
98	—	2	—	4	—	—	2	2	12	—	4	18	11	20	6	28	3	—	36	5	42	23	—	52	58	20	—	66	35	36	39	18	82	44	1	98
99	1	—	2	2	1	2	—	—	4	4	16	9	22	2	—	4	6	8	18	40	21	46	1	13	58	20	16	66	70	72	39	—	41	44	48	99
100	—	1	—	—	3	—	1	1	3	—	8	9	11	—	3	14	15	—	3	5	21	23	21	13	29	30	—	33	35	4	13	9	41	22	48	100

表 48　a 所属的指数，模 p 与模 p^{α}（续）

素数 p	最小原根 g	素数 p	最小原根 g	素数 p	最小原根 g
3	2	29	2	61	2
5	2	31	3	67	2
7	3	37	2	71	7
11	2	41	6	73	5
13	2	43	3	79	3
17	3	47	5	83	2
19	2	53	2	89	3
23	5	59	2	97	5

表 49　3至97各素数的最小原根

*　　　*　　　*

对某些给定的模，如果把具有同样主指数的底统统集中编组，则可看到一种奇妙关系. 我们将会发现，有着给定主指数 e 的底，其个数恰恰是 $\phi(e)$. 附表 50 就模 13 阐明了这一性质. [100]

$e=$

1	2	3	4	6	12
$1^1\equiv 1$	$12^2\equiv 1$	$3^3\equiv 1$	$5^4\equiv 1$	$4^6\equiv 1$	$2^{12}\equiv 1$
		$9^3\equiv 1$	$8^4\equiv 1$	$10^6\equiv 1$	$6^{12}\equiv 1$
					$7^{12}\equiv 1$
					$11^{12}\equiv 1$

表 50　模 13 的主指数

表 50 的最后一列明白显示，对素数模 p 来说，它有 $\phi(p-1)=\phi[\phi(p)]$ 个原根.

*　　　*　　　*

合数也能有原根. 若 x 的主指数是 $p-1=\phi(p)$，则称 x 是素数 p 的一个原根. 不管模 m 是素数还是合数，若在同余式 $x^{\phi(m)}\equiv 1 \bmod m$中，$\phi(m)$是 x 的主指数，则称 x 是 m 的原根. 可以证明，合数模的原根只能存在于以下若干种情形：(1)模是一个奇素数的乘幂；(2)一个奇素数乘幂的二倍；(3)合数 $m=4$，此时必有一个单一原根 3.

由第 12 章给出的定义，我们有

$$\phi(p^n) = p^{n-1}(p-1)$$

以及

$$\phi(2p^n) = \phi(2)\phi(p^n) = 1 \cdot p^{n-1}(p-1),$$

结果竟然相同.对 $49=7^2$ 这样的数我们将得出：

$$\phi(7^2) = 7^{2-1}(7-1) = 42.$$

查阅表 48 中 7^2 起头的那一列，我们发现底 3,5,10,12,17,24,26,33,38,40,45,47 的相应指数都是 42.因此以上这些整数全是 49 的原根.它们一共有 12 个，这是因为根据性质——属于指数 e 的底的个数应该是 $\phi(e)$，而

$$\phi(42) = \phi(2)\phi(3)\phi(7) = 1 \cdot 2 \cdot 6 = 12.$$

[101]

* * *

原根还有许多有趣性质，此处只能略加叙述.

1. 大于 3 的素数，其所有原根之乘积被该素数去除时，余数为 1.例如 13 有四个原根：2,6,7,11，其乘积为 924，它按模 13 同余于 1.

2. 若 p 为素数而 $p-1$ 能被一个平方数除尽，则原根之和能被 p 整除；但若 $p-1$ 不能被平方数整除，则要看$(p-1)$含有偶数还是奇数个素因子，各原根之和相应地得出$+1$或-1的余数.例如 $13-1=12$，它能被 4 除尽，此时便有 $2+6+7+11=26$，恰能被 13 整除.但对素数 11 而言，由于 $11-1=10$ 不能被平方数除尽，而 10 含有偶数个素因子，因而 11 的各原根之和 $2+6+7+8=23$ 除以 11 时，余数是$+1$.

3. 整数 3 恒为形如 $2^{2^n}+1$ 的素数的原根，但相应于 $n=0$ 的素数 3 例外.这意味着，当 $n=1,2,3,4$ 时，3 是 5,17,257,65537 诸相应素数的原根.

4. 若 $4n+1$ 是素数，则整数 2 是形如 $8n+3$ 的一切素数之

原根. 例如 $n=1$ 时,11 与 5 都是素数,所以 2 是 11 的原根. n 的下一个允许值是 7,而 2 是 59 的一个原根.

5. 若 q 为素数,则整数 2 是一切形如 $4q+1$ 的素数的原根. 例如,若 $q=3$,$4q+1=13$ 是素数,所以 2 是 13 的原根. 另外 $q=7$ 时,$4q+1=29$,而 2 也是素数 29 的原根.

6. 若 2^m+1 是一素数 p,则 p 的任一平方非剩余(参阅第 19 章)都是 p 的一个原根. 例如取 $m=4$,此时 $p=17$ 是一素数,它的平方非剩余是 3,5,6,7,10,11,12,14. 由表 48 可知,它们全都是 17 的原根.

7. 任一 $2^{4n}+1$ 的素数都有原根 7. 例如,取 $n=1$,则 17 有一原根为 7,而这在上面已经指出过了.

8. 如果对模 p 有一原根 g,则与 $p-1$ 互质的 $\phi(p-1)$ 个正整数都可用来作为 g 的指数,使所得之 g 的乘幂按模 p 与剩下的原根同余. 例如,3 是 17 的一个原根而 $\phi(16)=8$,与 16 互质的八个数为 1,3,5,7,9,11,13,15. 奇妙的是 $3^1,3^3,3^5,3^7,3^9,3^{11},3^{13},3^{15}$ 按模 17 分别同余于 3,10,5,11,14,7,12,6,而这些数全都是 17 的原根. [102]

参考文献

Cunningham, A. *Haupt-Exponents, Residue Indices, Primitive Roots*: London: F. Hodgson, 1922.

Jacobi, C. G. J. *Canon Arithmeticus*. Berlin, 1839.

Reid, L. W. *Elements of the Theory of Algebraic Numbers*. Baltimore: Johns Hopkins Press, 1946.

Shanks, W. "On the Number of Figures in the Period of the Reciprocal of Every Prime Number Below 20000," *Proceedings of the Royal Society of London*, **22**(1873), 200.

——. "Given the Number of Figures (Not Exceeding 100) in the Reciprocal of a Prime Number, to Determine the Prime

Itself," *Proceedings of the Royal Society of London*, **22** (1873), 381.

——. "On the Number of Figures in the Reciprocal of Every Prime Between 20000 and 30000," *Proceedings of the Royal Society of London*, **22**(1873), 384.

[103] Tchebycheff, P. L. *Theorie der Congruenzen*. Berlin, 1889.

第14章 不朽的三角形

实际上几乎人人知道 $3^2+4^2=5^2$，这是毕达哥拉斯定理的最简单应用. 该定理说：直角三角形两直角边的平方之和等于斜边的平方. 但较少的人知道 5，12，13，这些数同样能满足上述关系但又与 3，4，5 不成比例. 更少的人能给出第三个毕氏三角形的边长，又不同于上面已经提到过的两个，譬如说，7，24，25.

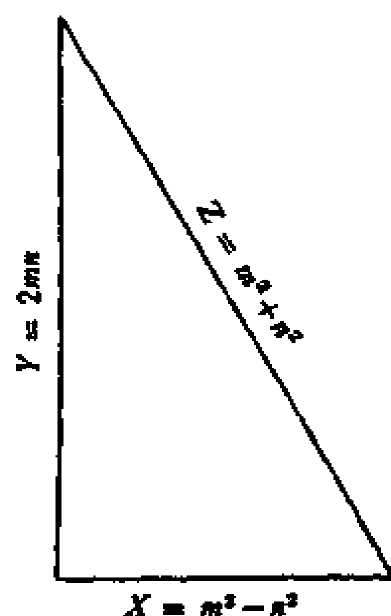


图 3 毕达哥拉斯三角形

具有整数边长的三角形一直是个有趣话题. 求两个整数，使其平方和是一平方数，不过是许多有趣问题之一而已. 除去 1 与 2 的平方之外，永远能找到至少一个平方数，把它加到一个已知平方数上去以后，其和仍是平方数. 值得注意的是，对于斜边，上

述说法不正确，对整数直角三角形来说，表示斜边的正整数必须是某种类型的数.

[104] 给出直角三角形整数边长的公式早在丢番图与早期希腊时代即已知晓，它们是：

$$\text{一条直角边：} X=m^2-n^2,$$
$$\text{另一直角边：} Y=2mn, \qquad \text{(公式 1)}$$
$$\text{斜　　边：} Z=m^2+n^2.$$

式中，数 m，n 是可以任取的正整数. 附表 51 给出了一些实例.

例子	m	n	$X=m^2-n^2$	$Y=2mn$	$Z=m^2+n^2$
1	2	1	3	4	5
2	3	2	5	12	13
3	5	2	21	20	29
4	9	6	45	108	117
5	5	3	16	30	34
6	4	3	7	24	25
7	6	1	35	12	37
8	18	17	35	612	613
9	9	8	17	144	145
10	4	1	15	8	17

表 51 "毕达哥拉斯"的三角形，即整数直角三角形

m 与 n 有时称为*母数*，如果我们把连续正整数对取作 m，n 值，即可得出表 52. 这时较大直角边 Y 与斜边 Z 是连续正整数.

母数		毕氏三角形的三边		
m	n	X	Y	Z
2	1	3	4	5
3	2	5	12	13
4	3	7	24	25
5	4	9	40	41
6	5	11	60	61
7	6	13	84	85

[105] **表 52 一直角边与斜边为连续数的毕氏三角形**

现在让我们把这两个直角边 X,Y 看作母数,于是我们得出表 53.

母数		毕氏三角形的三边		
m	n	X	Y	Z
4	3	7	24	$25=5^2$
12	5	119	120	$169=13^2$
24	7	527	336	$625=25^2$
40	9	1519	720	$1681=41^2$
60	11	3479	1320	$3721=61^2$
84	13	6887	2184	$7225=85^2$

表 53 斜边为平方数的毕氏三角形

[106] * * *

让我们对公式 1 再仔细察看一下.若两个数具有公因子,则它们的乘积,各次乘幂的和或差也应当具有该公因子.将这些事实应用于公式,我们发现,若 m、n 具有公因子,则三边 X,Y,Z 也应含有该公因子.另外,若 m,n 为偶数,或两者均为奇数,则 X,Y,Z 至少有个 2 作为公因子.如果我们想在 X,Y,Z 的数集中排除掉有公因子的数,就必须在 m 或 n 中选取一奇一偶(不同的奇偶性),而且没有公因子.作了这些限制后而得出的、具有整数边的直角三角形称为本原三角形,只需利用公式求出它们就行,因为一切非本原三角形都只要把前者的三边乘以任意整数即能得出.

要囊括一切毕氏三角形,公式 1 必须修改为:

$$X = K(m^2 - n^2),$$

$$Y = K(2mn), \qquad \text{(公式 1A)}$$

$$Z = K(m^2 + n^2).$$

若没有因子 K,某些非本原三角形,例如 9,12,15 就不能从公式 1 得出.有了公式 1A,令 $K=3$,$m=2$,$n=1$,上述非本原三角形马上就出来了.

从公式 1 能得出一切本原三角形,但只能得出三边的最高公因子是一个平方数,或平方数的二倍的那些非本原三角形.作为特例,该公式能给出三边边长只有公因子 2 的非本原三角形.若公因子是平方数的二倍,此时将产生一个值得注意的变换.由公式 1A:

$$X = 2L^2(m^2 - n^2),$$

$$Y = 2L^2(2mn),$$

$$Z = 2L^2(m^2 + n^2).$$

这些表达式可通过如下办法转变为公式1的形式：

$X=2L^2(m^2-n^2)=2(Lm+Ln)(Lm-Ln)=2MN$，

$Y=2L^2(2mn)=(Lm+Ln)^2-(Lm-Ln)^2=M^2-N^2$，

$Z=2L^2(m^2+n^2)=(Lm+Ln)^2+(Lm-Ln)^2=M^2+N^2$，

此处 $M=Lm+Ln$，$N=Lm-Ln$. 当 $L=1$ 时，变换更是特别引人注目. [107]

K 是一个平方数 L^2 时，不需变换，直接可得出：

$$X=L^2(m^2-n^2)=m^2L^2-n^2L^2,$$

$$Y=L^2(2mn)=2(mL\cdot nL),$$

$$Z=L^2(m^2+n^2)=m^2L^2+n^2L^2.$$

表51的第三例中，$m=5$，$n=2$ 没有公因子，而且一奇一偶，所以 X，Y，Z 是互质的. 对例4而言，由于 m，n 有公因子3，所以直角三角形的三边具有公因子9. 如果我们用公因子去除 m，n，结果即得出本原三角形5，12，13. 对例5来说，得出的是一个非本原三角形，因为 m，n 虽然互质，但它们的奇偶性相同，两者都是奇数，而非一奇一偶.

* * *

应当指出，对本原毕氏三角形的三个正整数而言，其中之一恒能被3整除，而另一个能被5整除. 两直角边之积恒能被12整除，而所有三边之乘积则能被60整除. 读者们自己很容易推导出这些关系.

* * *

我们现在要说明，在给出一个正整数时，怎样求出另一正整数，使两者之平方和恰为一正整数的平方. 给定数为奇为偶，解法是不一样的.

1. 当给定数 A 为奇数时：

把 A 分成两个因子.(若 A 为素数,这两个因子就是 1 与 A 的本身.)令较大的因子等于 $m+n$,较小因子等于 $m-n$,再解出 m,n 的两个联立线性方程,并代入公式以求出 X,Y,Z. 若要求出本原解,这两个因子必须互质.

设 $A=35$,令 $m+n=7$,$m-n=5$,便可求得 $m=6$,$n=1$,此时三边之长就是表 51 中的例 7. 若设 $m+n=35$,$m-n=1$,则得出的第二个解答就是例 8.

设 $A=17$,此时只能有 $m+n=17$,$m-n=1$,因为 17 是个素数,结果可得出例 9.

[108]

2. 当给定数 A 为偶数时:

可令 A 等于 $2mn$,此时 m,n 是任意两个相乘后能得到所需乘积的正整数. 若要求得本原解,A 必须能被 4 整除,并且 m,n 必须互质,还得有不同奇偶性. 如果 A 不能被 4 整除,则本原解不存在.

设 $A=8$,于是 $2mn=8$,$mn=4$. 令 $m=4$,$n=1$,结果可得出例 10 的三数组 15,8,17.

再设 $A=12$,于是 $mn=6$,若令 $m=6$,$n=1$,我们便得出例 7 的三数组;若令 $m=3$,$n=2$,便可得到例 2 的三数组.

*　　　*　　　*

毕氏三角形的问题许多世纪以来吸引着为数众多的数学家进行研究,此类问题的数量相当庞大,下面只是从中挑出了极少的一部分:

1. 若 A 是一个给定的正整数,有多少个本原三角形使它是一条直角边?

2. 若 A 是一个给定的正整数,不论本原或非本原,究竟有多少个毕氏三角形,使它是一条直角边?

3. 为了使一个正整数成为毕氏三角形(本原或非本原)的斜边,它必须取什么形式?有多少本原或非本原三角形使它能作为一条斜边?

4. 若 A 是一给定正整数，有多少直角三角形使之能成为一直角边或斜边？

5. 求一最小的正整数，使之能成为一定个数（例如有1000个）的直角三角形的直角边.

6. 求一正整数，使它能成为一斜边，或者直角边与斜边，而这样的直角三角形正好有1,000,000个.

7. 求出两直角边之差恰好等于1的毕氏三角形，并推导出能系统地求得它们的办法. 试求出前100个此类三角形. †[①]

8. 求出三个或更多个具有相等面积的毕氏三角形.

9. 求出具有最小周长而面积正好超过1,000,000的毕氏本原三角形. †

10. 求出三边边长在2000与3000之间的一个毕氏本原三角形. †

[109]

接下来的问题还有：面积为一定比值的毕氏三角形；周长是平方数的；面积与周长之和是立方数的；面积等于斜边的[②]；面积加上斜边的平方仍得出平方数的；周长等于一个给定数的. 总而言之，有关毕氏三角形的问题之多，简直无法列举.

在提出这些问题时，似乎很自然地想到再加上一个简单的条件：找出一个面积为平方数的毕氏三角形，但数学家们对此项寻求却是徒劳无功. 费马这位大师最后证明它是不可能的，也就是说，$mn(m^2-n^2)$ 不可能是平方数. 显然，上述问题是一个不定方程，在丢番图问题方面有点经验但以前从未碰到过这种面积问题的人，会产生一种强烈的诱惑，企图攻打它而不受到任何惩罚，他们总觉得迟早有一天会找到解决这个问题的小诀窍. 一般说来，他们的这些想法倒也并不离谱. 但此例不行，人们很快地陷入数字的流沙区域，迷失了目标. 后来总算是费马抛出了

① 有†号的问题在第26章有解法. ——原注.

② 这里均指的是在数值上相等的意思. ——译者注.

“无限递降法”，把他们拔出泥沼，恢复了信心. 然而，使用此种办法必须谨慎小心，因为在羊肠小径的两侧都长眠着一些不幸的数学家们的骸骨，他们企图穿越小径，可是却对它的制约未能给予足够注意.

证明一个关系式，例如 $mn(m^2-n^2)=K^2$ 不可能成立，费马的巧妙推理遵循着以下思路：假定存在着一些整数使此式成立；m 与 n 限于取某些形式. 代入并作简化以后，得出的方程同原先的非常相似，然而满足关系式的 p,q 却小于 m,n. 反复进行这种推理直至无限，于是得到越来越小的整数. 但是，对有限的整数 m,n 来说，比它们小的整数，只可能有有限多个. 这就引出矛盾，从而证明了原先假设的不可能. 对于此方法的详细说明，建议读者去参阅本书第 24 章中证明 $x^4+y^4=z^4$ 不成立的有关章节.

为什么数学中的某些关系可用直接证法，某些则非得用类似无限递降法之类的巧妙推理，此事尚不清楚.

*　　*　　*

让我们回到以前提出的问题. 表 51 的例 2 与例 7 给出了毕氏三角形的一边为 12 的两个解答. 例 7 与例 8 则对边 35 给出了两解. 例 9 与例 10 对 17 给出了两个解，其中一为直角边，一为斜边. 数 48 可以是 10 个不同毕氏三角形的直角边，如图 4 所示. [110]

任何形如 p^3q 的数(p,q 为奇素数)或 $16p$ 的数(p 为奇素数)正好有 10 个解；也就是说，可以是 10 个毕氏三角形的直角边. 据此说法，$3^3\cdot5=135$ 或 $16\cdot5=80$ 都有十解. 表 56 给出了可以是毕氏三角形的一边(直角边或斜边)的最小数 N，含此边的不同毕氏三角形数是一个指定数 T(T 从 1 到 100).

通常 N 只是一直角边；但有时经过适当选取后也可以包括斜边. 后者是在这样情况下选择的：对一个给定的 T 值，如只限于直角边时，得出的 N 值要较大一些，但若也包括斜边，则 N

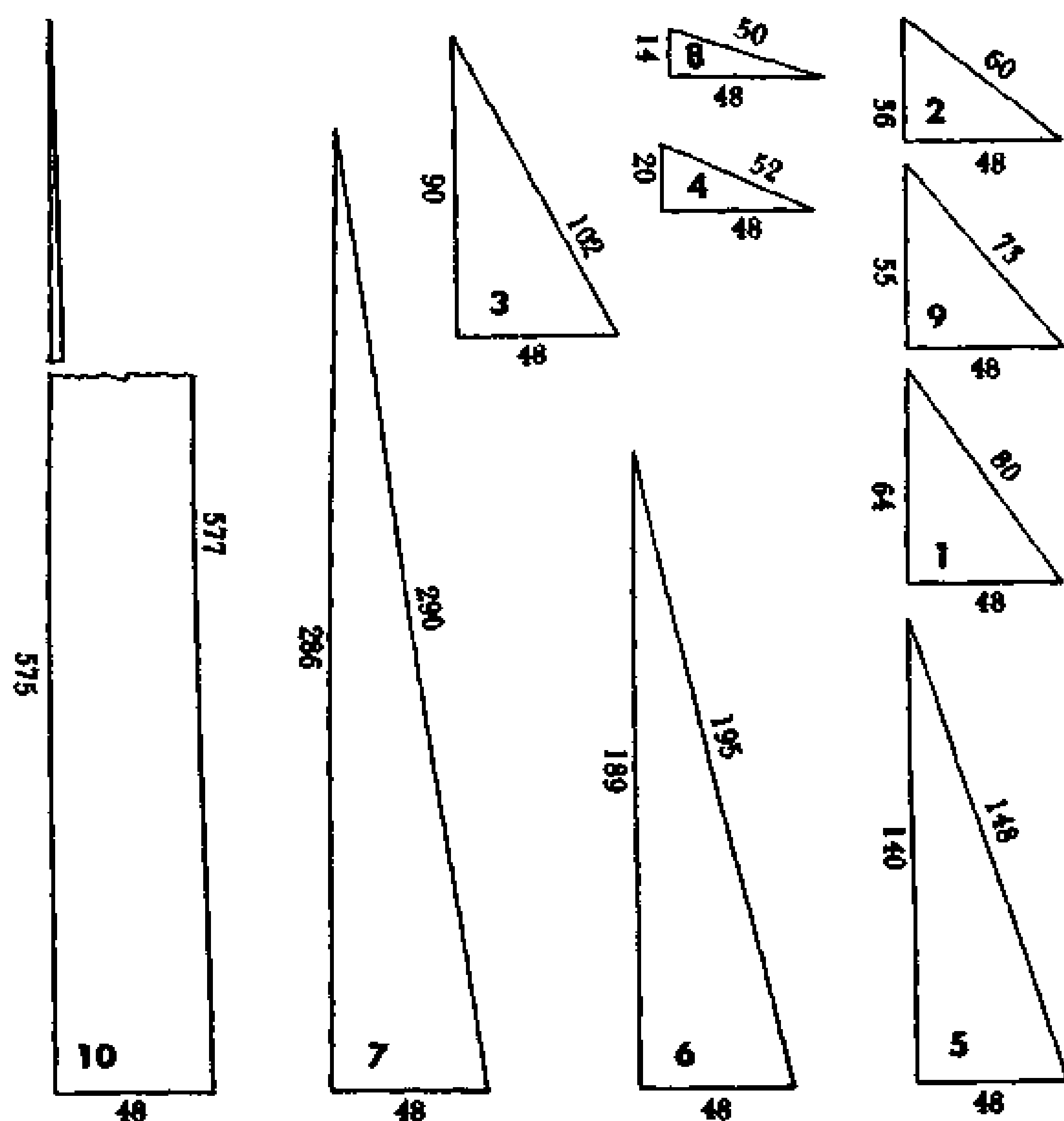


图 4 一条直角边等于 48 的十个毕氏三角形

值可以更小一些. 对 N 来说,如果其中至少含有一个 $4x+1$ 的素因子,则它可以是斜边,否则只能是直角边. 表中的 L 这一列给出了 N 是直角边的解的个数;H 列则给出了 N 是斜边的解的个数,因而 $L+H=T$. 例如,正好是两个不同毕氏三角形边长的最小数为 5;在第一解中,5 是作为直角边的(三数组 5,12,13),而在第二解中,5 是作为斜边的(三数组 3,4,5). 在该表中,三数组的确切数值未予列入. [111]

T	N	L	H
1	$3 = 3$	1	0
2	$5 = 5$	1	1
3	$2^4 = 16$	3	0
4	$2^2 \cdot 3 = 12$	4	0
5	$3 \cdot 5 = 15$	4	1
6	$5^3 = 125$	3	3
7	$2^3 \cdot 3 = 24$	7	0
8	$2^3 \cdot 5 = 40$	7	1
9	$3 \cdot 5^2 = 75$	7	2
10	$2^4 \cdot 3 = 48$	10	0
11	$2^4 \cdot 5 = 80$	10	1
12	$2^3 \cdot 3^2 = 72$	12	0
13	$2^2 \cdot 3 \cdot 7 = 84$	13	0
14	$2^2 \cdot 3 \cdot 5 = 60$	13	1
15	$2^{15} = 32768$	15	0
16	$2^6 \cdot 3 = 192$	16	0
17	$2^4 \cdot 3^2 = 144$	17	0
18	$2^{19} = 524288$	18	0
19	$2^7 \cdot 3 = 384$	19	0
20	$2^7 \cdot 5 = 640$	19	1
21	$3 \cdot 5^5 = 9375$	16	5
22	$2^3 \cdot 3 \cdot 7 = 168$	22	0
23	$2^3 \cdot 3 \cdot 5 = 120$	22	1
24	$2^2 \cdot 3 \cdot 5^2 = 300$	22	2
25	$2^9 \cdot 3 = 1536$	25	0
26	$2^3 \cdot 5 \cdot 13 = 520$	22	4
27	$2^6 \cdot 3^2 = 576$	27	0
28	$2^{10} \cdot 3 = 3072$	28	0
29	$3 \cdot 5^2 \cdot 13 = 975$	22	7
30	$2^{31} =$	30	0
31	$2^4 \cdot 3 \cdot 7 = 336$	31	0
32	$2^4 \cdot 3 \cdot 5 = 240$	31	1
33	$3 \cdot 5^8 =$	25	8
34	$2^2 \cdot 3 \cdot 5^3 = 1500$	31	3
35	$2^4 \cdot 5 \cdot 13 = 1040$	31	4
36	$2^{37} =$	36	0
37	$2^3 \cdot 3^2 \cdot 7 = 504$	37	0
38	$2^3 \cdot 3^2 \cdot 5 = 360$	37	1
39	$2^3 \cdot 3 \cdot 5^2 = 600$	37	2
40	$2^2 \cdot 3 \cdot 7 \cdot 11 = 924$	40	0
41	$2^2 \cdot 3 \cdot 5 \cdot 7 = 420$	40	1
42	$2^9 \cdot 3^2 = 4608$	42	0
43	$2^4 \cdot 5^5 = 50000$	38	5
44	$2^2 \cdot 3 \cdot 5 \cdot 13 = 780$	40	4
45	$2^7 \cdot 3^3 = 3456$	45	0
46	$2^{16} \cdot 3 = 196608$	46	0
47	$2^{10} \cdot 3^2 = 9216$	47	0
48	$2^7 \cdot 5^3 = 16000$	45	3
49	$2^6 \cdot 3 \cdot 7 = 1344$	49	0
50	$2^6 \cdot 3 \cdot 5 = 960$	49	1
51	$2^4 \cdot 5^6 = 250000$	45	6
52	$2^4 \cdot 3^2 \cdot 7 = 1008$	52	0
53	$2^4 \cdot 3^2 \cdot 5 = 720$	52	1
54	$2^4 \cdot 3 \cdot 5^2 = 1200$	52	2
55	$2^3 \cdot 3 \cdot 5^3 = 3000$	52	3
56	$2^{19} \cdot 5 =$	55	1
57	$2^{12} \cdot 3^2 = 36864$	57	0
58	$2^7 \cdot 3 \cdot 7 = 2688$	58	0
59	$2^7 \cdot 3 \cdot 5 = 1920$	58	1
60	$2^6 \cdot 3^5 = 15552$	60	0
61	$2^{21} \cdot 3 =$	61	0
62	$2^3 \cdot 3^2 \cdot 7^2 = 3528$	62	0
63	$2^{64} =$	63	0
64	$2^3 \cdot 3^2 \cdot 5^2 = 1800$	62	2
65	$3 \cdot 5^5 \cdot 13 = 121875$	49	16
66	$2^{10} \cdot 3^3 = 27648$	66	0
67	$2^3 \cdot 3 \cdot 7 \cdot 11 = 1848$	67	0
68	$2^3 \cdot 3 \cdot 5 \cdot 7 = 840$	67	1
69	$2^2 \cdot 3 \cdot 5^2 \cdot 7 = 2100$	67	2
70	$2^{24} \cdot 3 =$	70	0
71	$2^3 \cdot 3 \cdot 5 \cdot 13 = 1560$	67	4
72	$2^{15} \cdot 3^2 = 294912$	72	0
73	$2^4 \cdot 3^3 \cdot 7 = 3024$	73	0
74	$2^4 \cdot 3^3 \cdot 5 = 2160$	73	1
75	$2^4 \cdot 5^9 =$	66	9
76	$2^4 \cdot 3 \cdot 5^3 = 6000$	73	3
77	$2^9 \cdot 3 \cdot 5 = 7680$	76	1
78	$2^{79} =$	78	0
79	$2^{16} \cdot 5^2 =$	77	2
80	$2^3 \cdot 5 \cdot 13 \cdot 17 = 8840$	67	13
81	$3 \cdot 5^{20} =$	61	20
82	$2^6 \cdot 3^2 \cdot 7 = 4032$	82	0
83	$2^6 \cdot 3^2 \cdot 5 = 2880$	82	1
84	$2^6 \cdot 3 \cdot 5^2 = 4800$	82	2
85	$2^{10} \cdot 3 \cdot 7 = 21504$	85	0
86	$2^{10} \cdot 3 \cdot 5 = 15360$	85	1
87	$2^4 \cdot 3^2 \cdot 7^2 = 7056$	87	0
88	$2^{30} \cdot 3 =$	88	0
89	$2^4 \cdot 3^2 \cdot 5^2 = 3600$	87	2
90	$2^3 \cdot 3^2 \cdot 5^3 = 9000$	87	3
91	$2^4 \cdot 5^{11} =$	80	11
92	$2^{19} \cdot 3^2 =$	92	0
93	$2^9 \cdot 3^5 = 124416$	93	0
94	$2^4 \cdot 3 \cdot 7 \cdot 11 = 3696$	94	0
95	$2^4 \cdot 3 \cdot 5 \cdot 7 = 1680$	94	1
96	$2^{97} =$	96	0
97	$2^7 \cdot 3^2 \cdot 7 = 8064$	97	0
98	$2^4 \cdot 3 \cdot 5 \cdot 13 = 3120$	94	4
99	$2^7 \cdot 3 \cdot 5^2 = 9600$	97	2
100	$2^{34} \cdot 3 =$	100	0

表 56　可作为 T 个(T 是一个事先指定的数，其值可从 1 至 100)毕氏三角形一边的最小数 N

回到 $T=10$ 的情况，我们已找到 $48=16p$ 是个解，但由于 48 只含奇素数因子 3，而它不是 $4x+1$ 的形式，因此它不可能是条斜边. 但对 $N=80=16\cdot 5$ 来说，它的奇素数因子 5 是具有 $4x+1$ 形状的，因而 80 可以是一个毕氏三角形(三数组 48，64，80)的斜边. 对 $T=29$ 而言，最小数 975 是 22 个三角形的直角边，7 个三角形的斜边. 如果只要作为直角边的 29 个三角形，最小数的答案将是 $2^{30}=1073741824$，一个将近大出一百万倍的数.

表 57 给出的最小数是数以整百计的不同直角三角形的边；表 58 的性质与此类似，但不同直角三角形的个数更为庞大，是五十万的倍数. 请你想象一下有着五百万只直角三角形的巨大蜂窝，它们都有一条相同的边. 图 5A，5B，5C 画出了一只圆锯和两个星形，总数共有 23 个直角三角形，它们都有一条边等于 120. 作为直角边的有 22 种情况，作为斜边的只有一种情况.

现在让我们解决一下前面提出的问题. 设 60 是一个给定数，我们想知道使它为一条直角边的本原毕氏三角形究竟有多少个. 把 60 分解成质因数的连乘积，得出 $2^2\cdot 3\cdot 5$，于是 60 可以是 $2^{3-1}=4$ 个毕氏三角形的一直角边. 再看 5040，分成质因数 [115]

T	N	L	H
100	$2^{34}\cdot 3=$	100	0
200	$2^{10}\cdot 3^3\cdot 5=138240$	199	1
300	$2^9\cdot 3^2\cdot 5^3=576000$	297	3
400	$2^{45}\cdot 3\cdot 7=$	400	0
500	$2^{19}\cdot 3\cdot 5\cdot 7=$	499	1
600	$2^{601}=$	600	0
700	$2^{234}\cdot 3=$	700	0
800	$2^{21}\cdot 3^6\cdot 5=$	799	1
900	$2^4\cdot 3^2\cdot 5^8\cdot 7=$	892	8
1000	$2^{10}\cdot 3^2\cdot 5^3\cdot 7=$	997	3

表 57 可作为 T 个(T 为指定数，可从 100 至 1000)毕氏三角形一边的最小数 N

T	N	L	H
500000	$2^{19}\cdot3^{6}\cdot5\cdot7^{5}\cdot11^{3}\cdot19\cdot23$	499999	1
1000000	$2^{9901}\cdot5^{50}$	999950	50
1500000	$2^{180}\cdot3^{2}\cdot5^{278}\cdot7$	1499722	278
2000000	$2^{1000}\cdot3^{14}\cdot5\cdot7^{11}$	1999999	1
2500000	$2^{17}\cdot3^{6}\cdot5^{3}\cdot7^{5}\cdot11^{2}\cdot19\cdot23\cdot31$	2499997	3
3000000	$2^{271}\cdot3^{8}\cdot5^{426}$	2999574	426
3500000	$2^{14}\cdot3^{6}\cdot5\cdot7^{5}\cdot11^{3}\cdot13\cdot19^{3}\cdot23$	3499996	4
4000000	$2^{6634}\cdot3^{33}\cdot7\cdot11$	4000000	0
4500000	$2^{19}\cdot3^{6}\cdot5^{5}\cdot7^{3}\cdot11\cdot19\cdot23\cdot31\cdot43$	4499995	5
5000000	$2^{2324}\cdot3^{119}\cdot5\cdot7$	4999999	1
5500000	$2^{19}\cdot3^{5}\cdot5^{6}\cdot7^{3}\cdot11\cdot19\cdot23$	5499994	6
6000000	$2^{1279}\cdot3^{9}\cdot7^{9}\cdot11^{6}$	6000000	0
6500000	$2^{97}\cdot3^{8}\cdot5^{116}\cdot13^{8}$	6498020	1980
7000000	$2^{117}\cdot3^{30}\cdot5^{98}\cdot7^{2}$	6999902	98
7500000	$2^{1230}\cdot3^{74}\cdot5^{11}\cdot7$	7499989	11
8000000	$2^{79}\cdot3^{6}\cdot5^{33}\cdot7^{6}\cdot13\cdot17$	7999699	301
8500000	$2^{7210}\cdot3^{65}\cdot7\cdot11$	8500000	0
9000000	$2^{2722}\cdot3^{1653}$	9000000	0
9500000	$2^{19}\cdot3^{9}\cdot5^{3}\cdot7^{6}\cdot11^{5}\cdot13\cdot19\cdot23$	9499990	10
10000000	$2^{330}\cdot3^{44}\cdot5^{5}\cdot7^{15}$	9999995	5

表 58　可作为 T 个(T 为指定数,可从 500,000 到 10,000,000)毕氏三角形一边的最小数 N

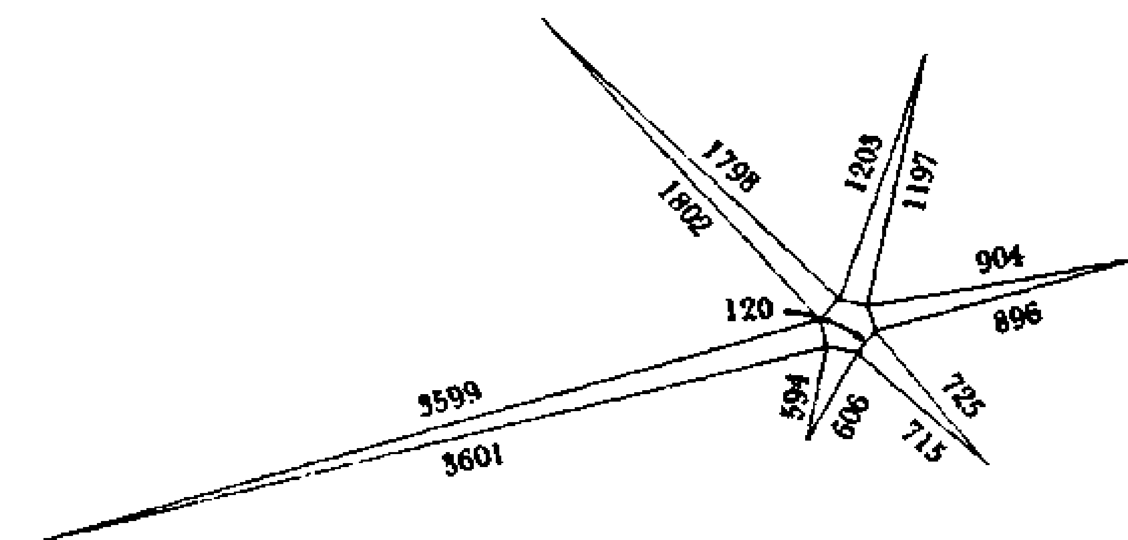


图 5A　有一边等于 120 的毕氏三角形

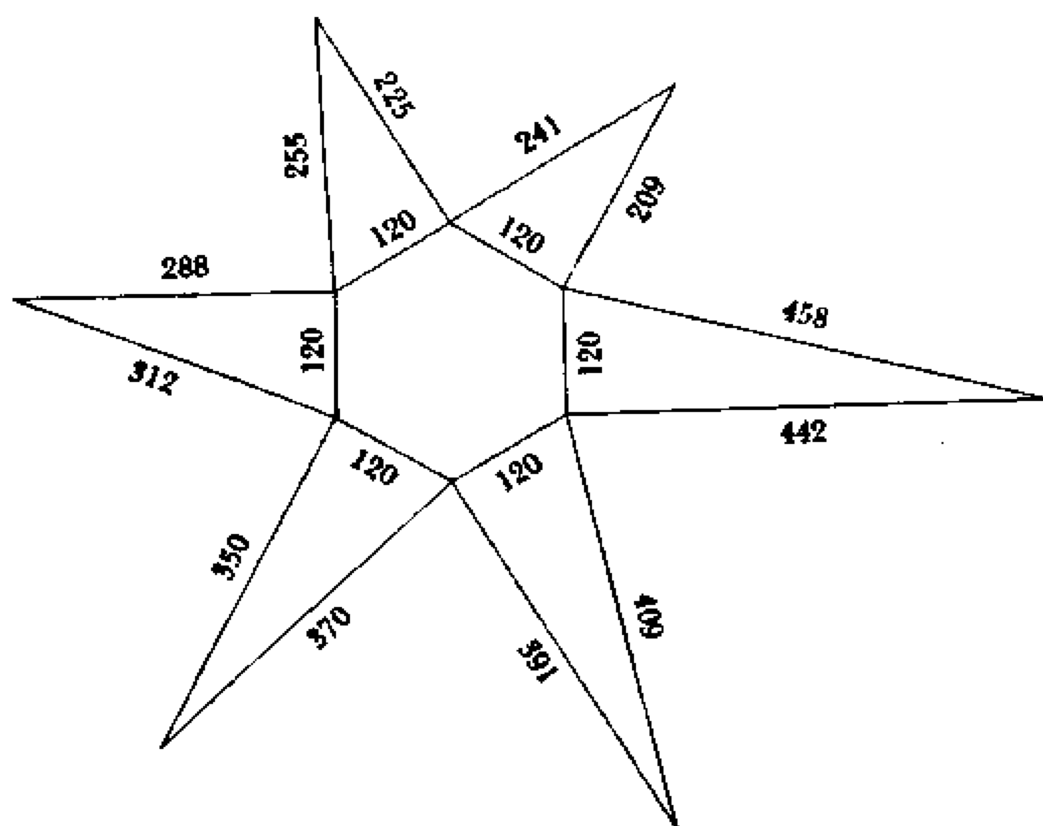


图 5B 有一边等于 120 的毕氏三角形

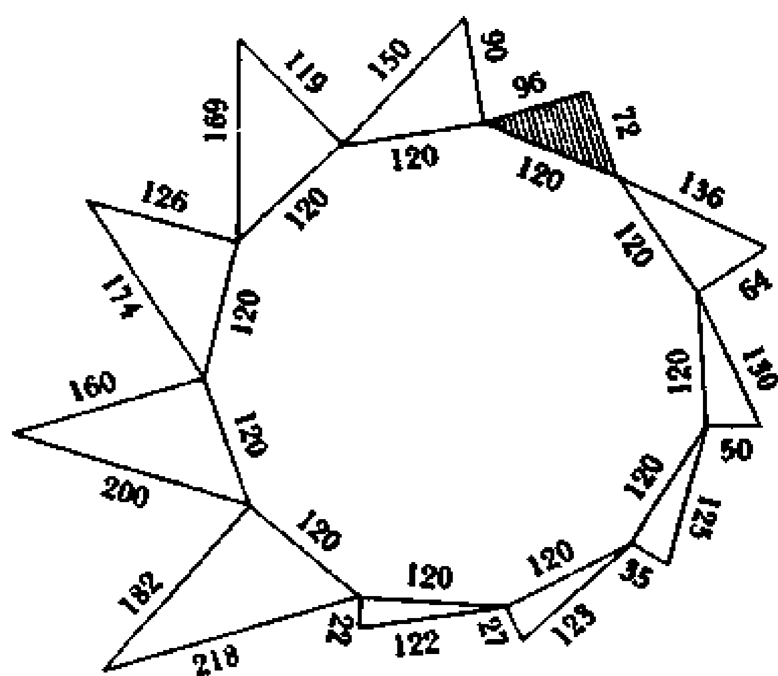


图 5C 有一边等于 120 的毕氏三角形

连乘积是 $2^4 \cdot 3^2 \cdot 5 \cdot 7$,一共有 4 个素数,$2^{4-1}=8$ 个解.一般地说,若某数含有 n 个素数或其乘幂,则它可能是 2^{n-1} 个本原毕氏三角形的一直角边,只有一个例外情况:若给定数为偶数但不能被 4 整除,那就没有解;例如 $30=2 \cdot 3 \cdot 5$ 不可能是本原三角形的一直角边,对形为 $4x+2$ 的任何数亦然.

*　　　　*　　　　*

对一个给定数 N,究竟有多少种办法使之成为本原或非本原毕氏三角形的直角边,为了解决这个问题,需要用上很不一样的办法.

若 $N=2^{a_0} p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$,则把 N 作为毕氏三角形直角边的方法总数为

$$L=\frac{(2a_0-1)(2a_1+1)(2a_2+1)\cdots(2a_n+1)-1}{2}.$$

(公式 2)

对 $60=2^2 \cdot 3 \cdot 5$ 来说,把后面两个因子的每个指数乘上 2 再加 1,但对 2 的指数却是乘 2 减 1,于是即有:

$$\frac{(2\cdot 2-1)(2\cdot 1+1)(2\cdot 1+1)-1}{2}=\frac{3\cdot 3\cdot 3-1}{2}=13.$$

对 $30=2 \cdot 3 \cdot 5$ 来说,结果是

$$\frac{(2\cdot 1-1)(2\cdot 1+1)(2\cdot 1+1)-1}{2}=4.$$

而对 $45=3^2 \cdot 5$,结果是

$$\frac{(2\cdot 2+1)(2\cdot 1+1)-1}{2}=7.$$

*　　　　*　　　　*

对问题 3 而言,只有能归结为 $K(m^2+n^2)$ 的数才有可能是本原或非本原毕氏三角形的斜边.任何正整数,只要它至少含有

一个 $4x+1$ 形式的素数除数，例如 5，10，13，15 等，则必能如此表达. 但作为本原三角形的斜边，必须将 K 值限定为 1，于是 m [116] 与 n 必然是互质的，而且奇偶性也不同. 作为本原三角形，只有每个素除数都取 $4x+1$ 时才能满足这些要求，例如 5，13，65，85 等等. 形为 $4x-1$ 的素数(如 3，7，11，19 等)不应作为该数的因子. 若某数 N 有 n 个不同素因子，而每个素因子又都是 $4x+1$ 形状的，则 N 可以是 2^{n-1} 个本原毕氏三角形的斜边. 例如，$65=5\cdot13$ 可以是 $2^{2-1}=2$ 个毕氏三角形的斜边；$1105=5\cdot13\cdot17$ 可为 $2^{3-1}=4$ 个这类三角形的斜边. 然而 15，21，39 是不行的，因为至少有一个除数 3 不符合规定的形式.

若

$$N = 2^{a_0} p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r},$$

这里 p_i 是形为 $4x-1$ 的素数，q_i 是形为 $4x+1$ 的素数，则 N 甚至连一个本原三角形的斜边都不是，但它可能是

$$H = \frac{(2b_1+1)(2b_2+1)\cdots(2b_r+1)-1}{2} \quad (\text{公式 } 3)$$

个非本原三角形的斜边. 同样的公式也可以应用到直角边场合，但此时不是看全部素数，而只要去考虑那些形为 $4x+1$ 的素数.

设 $N=2^5\cdot3\cdot5\cdot7^5\cdot11^3\cdot13^2$，不考虑素数 2，3，7，11，只要考虑 5 与 13 的指数，于是就得：

$$H = \frac{(2\cdot1+1)(2\cdot2+1)-1}{2} = 7,$$

所以 N 只能是七个毕氏三角形的斜边，但若考虑的是直角边，则有

$$\frac{(2\cdot5-1)(2\cdot1+1)(2\cdot1+1)(2\cdot5+1)(2\cdot3+1)(2\cdot2+1)-1}{2}$$
$$=15592$$

个毕氏三角形，所以一共有 15599 个毕氏三角形，使 N 为直角边或斜边. 把 N 作为斜边的本原三角形甚至连一个都没有，因为并不是每一个素数除数都具有 $4x+1$ 的形式.

[117] * * *

问题 5 是问题 2 的逆. 由公式 2 可得

$$2L+1=(2a_0-1)(2a_1+1)(2a_2+1)\cdots(2a_n+1),$$

这就使下列步骤的理由变得很明瞭：给定一数 L，试求另一数 N（尽量希望是最小者），使它是 L 个毕氏三角形的直角边. 将 $2L+1$ 分解因子，得出 $c_0, c_1, c_2, c_3, \cdots, c_n$，这些因子并不要求都不一样，也不必非为素数不可. 然后算出 $a_0=(c_0+1)/2$，$a_1=(c_1-1)/2$，$a_2=(c_2-1)/2$，$a_3=(c_3-1)/2$，$\cdots$，$a_n=(c_n-1)/2$. 于是 $N=2^{a_0}p_1^{a_1}p_2^{a_2}p_3^{a_3}\cdots p_n^{a_n}$ 便是本问题的一个解，这里的素数 p 可由人们自由选取. 一般地说，用以下办法可获得较小的解答（但并非永远如此）：先把 $2L+1$ 分解成相同或相异素数的一次幂，并按由小到大递增的素数 $2, p_1, p_2, p_3, \cdots, p_n$ 来分别安排其指数 $a_0, a_1, a_2, a_3, \cdots, a_n$，指数值则按递减顺序来分先后.

例 1. 试求出一个正整数 N，使它正好是 52 个毕氏三角形的直角边. 此处，$2L+1=105=7\cdot5\cdot3$. 分别算出 $a_1=(7-1)/2=3$，$a_2=(5-1)/2=2$，$a_3=(3-1)/2=1$；于是由关系式 $N=p_1^3p_2^2p_3$ 给出的任意数 N 都是问题的解. 若 $p_1=3$，$p_2=5$，$p_3=7$，这将给出 $N=3^3\cdot5^2\cdot7=4725$. 如果改为取素数 2，3，5，此时将得出 $N=2^4\cdot3^2\cdot5=720$，2 的指数将增加 1，因为此时将不用 $a_1=3$，代替它的是 $a_0=(7+1)/2=4$. 由于 5 也是一个因子，所以 N 也有可能是某一毕氏三角形的斜边，如想排除此种可能性，那就可用 7 来代替 5，从而得出 $N=2^4\cdot3^2\cdot7=1008$，这就是表 56 中相应于 $T=52$ 的 N 数据. 之所以不用更小的数据 720，因为它实际上是 53 个毕氏直角三角形的边，其中有 52 三角形是将 720 作为一直角边，而有 1 个三角形是将 720 作为

斜边的. 事实上,数 720 的确是 $T=53$ 时的解,这在表中也能看得到.

这里有一个注意点与最小解有关. 把 $2L+1$ 分解成素数因子的一次乘幂不一定永远能得出最小解,即便指数 $a_0,a_1,a_2,a_3,\cdots,a_n$ 按照最有利的方式指派给各个素数也是如此. 譬如说,$L=121$,则 $2L+1=243=3\cdot3\cdot3\cdot3\cdot3$,$a_1=a_2=a_3=a_4=1$,$a_0=(3+1)/2=2$,此时 $N=2^2\cdot3\cdot5\cdot7\cdot11$ 像是能得到最小解了. 但若把 $2L+1$ 分解成 $9\cdot3\cdot3\cdot3$,则 $a_0=5$,$a_1=a_2=a_3=1$,而 $N=2^5\cdot3\cdot5\cdot7$ 要比上一解更小. 此种较少出现的情况发生在 $2L+1$ 由许多小素数组成时,$2L+1=p_1p_2p_3\cdots p_k$,k 个素数都以一次幂形式出现,可以相同也可以相异,p_1 不小于 p_2,p_2 不小于 p_3,……,且 $2^{(p_1p_2-p_1)/2}$ 小于 $P^{(p_k-1)/2}$,这里的 P 是从 2 算起的第 k 个素数. 譬如,在上例中,$p_1=p_2=3$;$k=5$;$P=11$,而 2^3 却小于 11. [118]

例 2.　设 $L=1000$,则 $2L+1=2001=29\cdot23\cdot3$,$a_1=14$,$a_2=11$,$a_3=1$. 一般解为 $p_1^{14}p_2^{11}p_3$;而最小解是 $2^{15}\cdot3^{11}\cdot5$. 若所求之数也可作为斜边长,则可得到比它小得多的解答,表 57 中已经给出,后文也将提到.

*　　　*　　　*

问题 6 的第一部分可以像问题 5 那样去求解,但与所求解数有关的素数都应具有 $4x+1$ 形式. 2 的乘幂或 $4x-1$ 形式的素数可以自由穿插而不致影响其结果. 作为正好是 1000 个毕氏三角形的斜边,答案是 $5^{14}\cdot13^{11}\cdot17$(见上面的例 2). 当然,在 1000 个毕氏三角形中,此数也有可能作为直角边. 在数 $5^{14}\cdot13^{11}\cdot17$ 乘上 2 的任意次幂或 $4x-1$ 形的素数不会改变以它作为斜边的毕氏三角形的个数.

问题 6 的第二部分,即要找出一个数来,使它是具有给定个数的毕氏三角形的斜边或直角边. 此种提法相当有趣,因为,只要允许收入为数寥寥的、可作为斜边的解法,相应的解答可以远

远小于只能用作直角边的 N 数.

设

$$N = 2^{a_0} p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r},$$

利用公式 2 与公式 3,我们即有

$$2L + 1 = (2a_0 - 1)(2a_1 + 1)(2a_2 + 1)\cdots(2a_n + 1) \times (2b_1 + 1)(2b_2 + 1)\cdots(2b_r + 1), \quad (\text{公式 } 4)$$

$$2H + 1 = (2b_1 + 1)(2b_2 + 1)\cdots(2b_r + 1).$$

若 Q 是这两式的比值,T 为 L 与 H 之和,在消去 L 之后,可得 $(2H+1)(Q+1)=2(T+1)$. 显然 $(2H+1)$ 永为奇数,因而 $(Q+1)$ 必须是偶数而 Q 为奇数.

于是就提示了以下具体步骤:设 T 是要求的可作为直角边或斜边的毕氏三角形的解数. 把 $2(T+1)$ 分成一对因子 A 与 [119] B,A 奇 B 偶. 一般说来,这有多种安排方法,而其中的每一个都可以提供一型解. 这些因子于是分别对应于 $(2H+1)$ 与 $(Q+1)$.

把 A 分解为因子 $d_1 \geqslant d_2 \geqslant d_3 \geqslant \cdots \geqslant d_r$,并解出 $b_1=(d_1-1)/2$,$b_2=(d_2-1)/2$,$\cdots$,$b_r=(d_r-1)/2$. 这些是作为指数,安排到 $4x+1$ 形式的素数 q 上面去的. 为了求得最小解,需将 b_i 按递减顺序,q_i 按递增顺序布置. 由 $B=Q+1$,求出 Q,把 Q 分解成因子:

$$c_0 \geqslant c_1 \geqslant c_2 \geqslant c_3 \geqslant \cdots \geqslant c_n,$$

并求出 $a_0=(c_0+1)/2$,$a_1=(c_1-1)/2$,$a_2=(c_2-1)/2$,$a_3=(c_3-1)/2$,$\cdots$,$a_n=(c_n-1)/2$. 并将 a_0 作为素数 2 的指数,其余的 a_1,a_2,$\cdots$,a_n 作为 $4x-1$ 形式素数的指数.

在 $Q=1$ 时,a_0 将是 1,而 $a_1=a_2=\cdots=a_n$ 将是 0,于是 $N=2q_1^{b_1}q_2^{b_2}\cdots q_r^{b_r}$. 作为边(直角边或斜边),此数正好与 $N=q_1^{b_1}q_2^{b_2}\cdots q_r^{b_r}$ 完全一样,它们所对应的毕氏三角形的个数是相同的,此

点可由公式4予以证明.因此,如果人们的兴趣限于最小解,则前者可以舍弃,只用后者.由于$Q=1$时,$L=H$,所以作为直角边的毕氏三角形个数与作为斜边的毕氏三角形个数正好完全一样.

例3. 试求出一个数,它正好是1000个不同毕氏三角形的斜边或一直角边,并求出此类数中的最小者.此处$T=1000$,$2(T+1)=2002$,2002的奇数除数$A=2H+1$已在表59中给出,表中也给出了此等除数的因子$d_1,d_2,\cdots,d_r$以及与之相应的指数$b_1,b_2,\cdots,b_r$.$Q=B-1$的值及其因子$c_0,c_1,c_2,\cdots,c_n$也同时给出.最后可以得出$a_0,a_1,a_2,\cdots,a_n$等指数以及通过选定素数而得出的解(其中也包括了最小解).

表59中的第5解是最小解,此时$2H+1=7$,所以$H=3$,因此共有三个毕氏三角形,$2^{10}\cdot 3^2\cdot 5^3\cdot 7$是作为斜边的,而在其余的997个直角三角形中,该数是作为一条直角边的.请把这个答案同例2的$2^{15}\cdot 3^{11}\cdot 5$对比一下,后面的数字较大,这是由于最小解只限于直角边的缘故.

如果$T+1$是2的乘幂,因为没有奇除数,结果就不可能有任何H解.作为此种情况的一个实例,我们来求一个数N,它是63个毕氏三角形的斜边或一直角边.这里$T=63$,且

$$2(T+1)=2\cdot 64=1\cdot 128=(2H+1)(Q+1),$$ [120]

从而$2H+1=1$,$H=0$,$Q=127$,$N=2^{64}$或$p_1{}^{63}$,这里的p_1是$4x-1$形式的素数.前一解是最小解.对p_1,不能令它取值5,也不能用其他$4x+1$形式的素数值,因为如果那样的话,将会有63个"斜边"解,再加上63个"直角边"解,总数将是126,整整翻了一番.

例4. 给定$T=1000000$,求最小解.表59也已经指出步骤.此时将有50个斜边解.

此时的最小解是$2^{9901}\cdot 5^{50}$,有50个直角三角形是把此数作

解的类型序号	2(T+1)的因子对	$A=2H+1=$奇数因子	A的因子 $d_1,d_2,\cdots,d_r$	指数 $b_1,b_2,\cdots,b_r$	$B-1=Q$	Q的因子 $c_0,c_1,c_2,\cdots,c_n$	指数 $a_0,a_1,a_2,\cdots,a_n$	最小解
1	1001·2	1001	13·11·7	6,5,3	1	1	1	$5^6\cdot13^5\cdot17^3$
2	77·26	77	11·7	5,3	25	5·5	3,2	$2^3\cdot3^2\cdot5^5\cdot13^3$
3	91·22	91	13·7	6,3	21	7·3	4,1	$2^4\cdot3\cdot5^6\cdot13^3$
4	143·14	143	13·11	6,5	13	13	7	$2^7\cdot5^6\cdot13^5$
5*	7·286	7	7	3	285	19·5·3	10,2,1	$2^{10}\cdot3^2\cdot5^3\cdot7$
6	11·182	11	11	5	181	181	91	$2^{91}\cdot5^5$
7	13·154	13	13	6	153	17·3·3	9,1,1	$2^9\cdot3\cdot5^6\cdot7$

可作为 $T=1000$ 个不同毕氏三角形一边的数

解的类型序号	2(T+1)的因子对	$A=2H+1=$奇数因子	A的因子 $d_1,d_2,\cdots,d_r$	指数 $b_1,b_2,\cdots,b_r$	$B-1=Q$	Q的因子 $c_0,c_1,c_2,\cdots,c_n$	指数 $a_0,a_1,a_2,\cdots,a_n$	最小解
1	1000001·2	1000001	9901·101	4950,50	1	1	1	$5^{4950}\cdot13^{50}$
2	9901·202	9901	9901	4950	201	67·3	34,1	$2^{34}\cdot3\cdot5^{4950}$
3*	101·19802	101	101	50	19801	19801	9901	$2^{9901}\cdot5^{50}$

有*号者为最小解.

可作为 $T=1000000$ 个不同毕氏三角形一边的数

表 59

为斜边的(因为 $2H+1=101$),而有 999950 个三角形把它作为直角边.

如 1000000 只算直角边解个数,此时将有 $2000001=666667\cdot 3$,第一因子是个素数.于是指数为 333333 及 1,由此而产生的解是 $p_1^{333333}p_2$,最小解为 $2^{333334}\cdot 3$.同 $2^{9901}\cdot 5^{50}$ 相比,这是一个大得很多的数目.

*　　　*　　　*

在问题 7 中,加上去的条件是毕氏三角形的直角边一定要是连续正整数.显然,3,4,5 三角形能满足此条件;碰得正巧,这三边恰好能构成连续数.除此孤例以外,其他三角形均不能出现三边为连续数的现象,这是由于:如果 $m^2-n^2=X$,$2mn=X+1$,$m^2+n^2=X+2$,则由加法运算,可得 $m^2=X+1$,再由减法运算,可得 $n^2=1$,这将使 $2mn=m^2$,即 $2n=m$,但因 $n=1$,于是 $m=2$,而 $X=3$,结果依然是唯一解 3,4,5.

如果只要求直角边是连续数,则或者是

$$m^2-n^2+1=2mn,$$

或者是

$$2mn+1=m^2-n^2.$$

由前一关系式得出 $(m-n)^2=2n^2-1$,后一关系式得出 $(m-n)^2=2n^2+1$.两者可合并为一式:$(m-n)^2=2n^2\pm 1$,从而有 $(m-n)^2-2n^2=\pm 1$.一个平方数减去另一平方数的 k 倍等于 ± 1,这种类型的方程称为佩尔方程,在数论爱好者中间它是负有盛名的.关于佩尔方程的讨论将在本书后面章节中进行;目前我们只打算通过试探办法找到 n 的一些值,以使得 $2n^2\pm 1$ 为一个平方数.这些数值形成一个级数:1,2,5,12,29,70,169,…,加号与减号交替使用,开始时用减号.与之相应的平方数 $(m-n)^2$,m 值以及前十个毕氏三角形的直角边与斜边都已在表 60 中给出.　[122]

序号 r	n	$2n^2\pm1=(m-n)^2$	$m-n$	m	$X=m^2-n^2$	$Y=2mn$	$Z=m^2+n^2$
1	1	1	1	2	3	4	5
2	2	9	3	5	21	20	29
3	5	49	7	12	119	120	169
4	12	289	17	29	697	696	985
5	29	1681	41	70	4059	4060	5741
6	70	9801	99	169	23661	23660	33461
7	169	57121	239	408	137903	137904	195025
8	408	332929	577	985	803761	803760	1113689
9	985	1940449	1393	2378	4684659	4684660	6625109
10	2378	11309769	3363	5741	27304197	27304196	38613965

表 60 两直角边为连续数的毕氏三角形

在此表中，可以观察到一些有趣关系．例如，m 的值就是 n 的值，但超前一步，即 $m_r=n_{r+1}$. m 或 n 的即时值都可从前一值的二倍再加上更前面一值而得到．例如，$12=2\cdot5+2$；$29=2\cdot12+5$，等等；一般有 $n_r=2n_{r-1}+n_{r-2}$. 还可以看到，斜边的相继各值在 m 列中都是有的，一般有关系式 $Z_r=m_{2r}$.

可以推导出更有用的公式来直接计算 X,Y,Z，而不必把 m 与 n 都列举出来．注意到表 60 中，X 与 Y 交替地出现一个比另一个大 1 的情况，如果不用这种办法，我们在纵列中只列出两条直角边中的较小者，

序号	A	Z
1	3	5
2	20	29
3	119	169
4	696	985
5	4059	5741

这个纵列称为 A 列，而将斜边的一列仍旧叫做 Z 列，同以前一样，则有关系式 $A_r=6A_{r-1}-A_{r-2}+2$，$Z_r=6Z_{r-1}-Z_{r-2}$. 例如，在第五个直角三角形中有 $r=5$，$A_r=4059$；$A_{r-1}=696$；$A_{r-2}=119$；而 $4059=6\cdot696-119+2$. 类似地有 $Z_r=5741$；$Z_{r-1}=985$；

$Z_{r-2}=169$，而 $5741=6\cdot985-169$. 于是，紧随其后的三角形边长即可迅速地算出来，下面再给出一个可用于检验数据是否正确的式子：$A_r+A_{r-1}+Z_{r-1}+1=Z_r$，例如，$4059+696+985+1=5741$. [123]

读者们或许愿意证明以上三个关系式，并继续推算 20 个或更多的两直角边是连续数的毕氏三角形. 本书作者已计算了前 100 个这类三角形. 最后一个三角形的较小的直角边与斜边已在此处特别刊出，如果读者们也想来计算一下，从第 11 个到第 100 个，也许它是一个极大的精神支持. 如果他在半途丧失信心，那么他可以参看第 26 章并找到数达 100 个之多的全部答案.

$$A_{100}=21669693148613788330547979729286307164015202768699465346081691992338845992696,$$
$$Z_{100}=30645573943232956180057972969833245887630954508753693529117371074705767728665.$$

直角边由一个 77 位数表示的三角形基本上是一个极其精确的 45°角的等腰直角三角形. 每只锐角与 45°角之间的差异，正如人们所预期的那样，小得微乎其微，但如果构成此角的两条边延长得足够远，最终也许会相当散开. 一个电子的直径大约是 $8\cdot10^{-14}$英寸，现在设想可测空间的外部限制为一千亿光年，这个数据要比巴洛摩山上的 200 英寸望远镜以及加利福尼亚州大松树市的最新射电望远镜能观测到的宇宙范围着实大出许多倍. 所谓一光年，是光以每秒 186,300 英里的速度在一年中所走的距离，因而大致等于 $186300\cdot60\cdot60\cdot8765$ 英里(每年大约有 8765 小时强)，亦即六万亿英里($6\cdot10^{12}$英里). 上述那个极其渺小的角的两边，即使延长到宇宙的尽头(大约 $6\cdot10^{23}$英里)，再把一个电子无限分割(如果那是可能的话)——或者把一个氢原子核(它只有氢原子的$\frac{1}{2000}$那么大)分成极小极小的球

体，其数量比地球上所有水滴的总数还要多得多. 纵然如此，上述那只小角两边之间留出的空隙，依旧容纳不下一只超小球体！因此，我们最好还是把这种百分之一的稀有事件[①]说成是一个正好 45°角的等腰直角三角形，心安理得地放它过关.

*　　*　　*

第 r 条直角边与斜边可以用公式表示为 r 的函数而直接算出，不必依靠"循环"级数. 但此种公式不切实际，因为计算起来极为繁复. 公式如下：

[124]

$$A_r=\frac{(\sqrt{2}+1)^{2r+1}-(\sqrt{2}-1)^{2r+1}}{4}-\frac{1}{2},$$

$$Z_r=\frac{(\sqrt{2}+1)^{2r+1}+(\sqrt{2}-1)^{2r+1}}{2\sqrt{2}}.$$

令 $r=1,2$，于是有：

$$A_1=\frac{(\sqrt{2}+1)^3-(\sqrt{2}-1)^3}{4}-\frac{1}{2}=3,$$

$$Z_1=\frac{(\sqrt{2}+1)^3+(\sqrt{2}-1)^3}{2\sqrt{2}}=5;$$

$$A_2=\frac{(\sqrt{2}+1)^5-(\sqrt{2}-1)^5}{4}-\frac{1}{2}=20,$$

$$Z_2=\frac{(\sqrt{2}+1)^5+(\sqrt{2}-1)^5}{2\sqrt{2}}=29.$$

对 A 与 Z 的其他值，即使 r 的数值相对说来很小，计算量的增大依然非常显著.

计算两直角边为连续数的毕氏三角形，有一种方法较为简便，可以使用下列规则：若 m,n 为此种毕氏三角形的母数，而

① 统计学里有两种置信限，一为 5%，一为 1%，此处属于后一种. 低于百分之一的概率，在实际生活中通常已被认为稀有之事. ——译者注.

$m>n$，则 $2m+n,m$ 将能产生另一个此类三角形. 例如 3,4,5 三角形的母数为 $m=2,n=1$；则以 5 与 2 为母数，将可得出 21，20，29；再下一对母数是 12 与 5，它们可以得出三角形 119，120，169，等等，依此类推.

* * *

一个远为简单的问题是直角边与斜边是连续整数的毕氏三角形的决定. 由此可得或者是 $m^2-n^2+1=m^2+n^2$ 或者是 $2mn+1=m^2+n^2$. 第一式无正整数解，因那时 n 将为无理数. 由第二式可得 $m^2-2mn+n^2=1$. 即 $(m-n)^2=1$，于是 $m=n+1$. 因此，只要 m 与 n 是连续整数，斜边必然比偶数的那一直角边大 1，当然，这只有在一个本原毕氏三角形中才有可能实现.

* * * [125]

毕氏三角形的面积显然等于 $mn(m^2-n^2)$. 在问题 8 中，要求我们求出面积相等的三个毕氏三角形，也就是需要求出以下方程的整数解：

$$mn(m^2-n^2)=pq(p^2-q^2)=tu(t^2-u^2).$$

这是丢番图分析（不定方程或不定分析）中的问题，有许多种方法求解. 图 6 所示的三个三角形都能满足上述关系式.

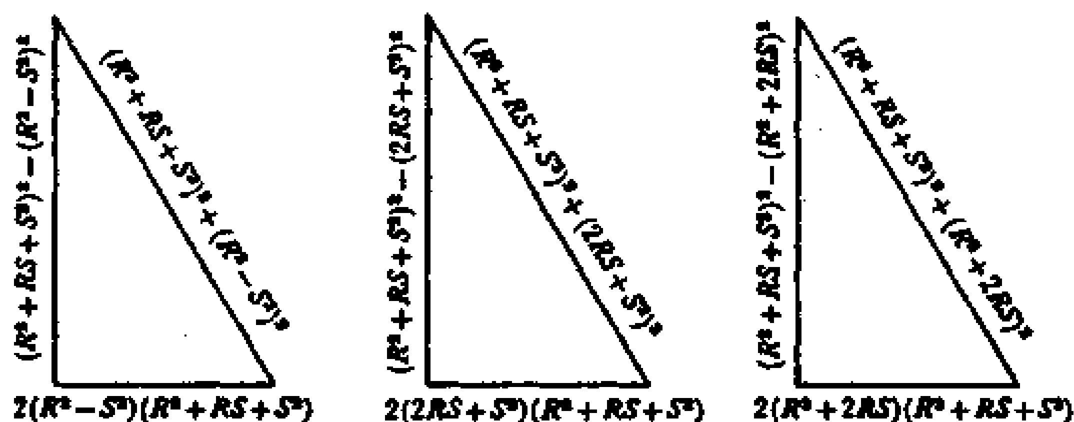


图 6 有相等面积的毕氏三角形

此解对应于：

$$m = r^2 + rs + s^2,\quad p = m = r^2 + rs + s^2,\quad t = r^2 + 2rs,$$
$$n = r^2 - s^2,\qquad q = 2rs + s^2,\qquad u = r^2 + rs + s^2.$$

公共面积等于 $rs(2r+s)(r+2s)(r+s)(r^3-s^3)$.

若 $r=2, s=1$,于是得出三个数组(40,42,58);(24,70,74);(15,112,113)以作为毕氏三角形的三边,其中每一个三角形的面积都等于 840. 若 $r=3, s=1$,得出的三数组为(105,208,233);(120,182,218);(56,390,394);每一个三角形的面积都是 10920.

费马利用一种简单办法来求得两个等积的毕氏三角形. 设 a, b 是两条直角边,c 是斜边,则有关系式 $a^2+b^2=c^2$,他用 $m=c^2, n=2ab$ 作为一个新的毕氏三角形的母数,从而得出后者的直角边:$m^2-n^2=c^4-4a^2b^2=(a^2-b^2)^2$, $2mn=4c^2ab$,以及斜边 $m^2+n^2=c^4+4a^2b^2$. 其面积等于 $2c^2ab(c^4-4a^2b^2)=2c^2ab(a^2-b^2)^2$. 显然,此三角形与把 a, b, c 各乘以 $2c(a^2-b^2)$ 所获的三角形是等积的. 这很容易证明;后面这个"放大"过的三角形的两条直角边是 $a\cdot 2c(a^2-b^2)$ 与 $b\cdot 2c(a^2-b^2)$,其面积显然等于 $2c^2ab(a^2-b^2)^2$.

[126]

如取 $a=4, b=3, c=5$,则母数为 $m=25, n=24$,形成的三角形之各边长是 49,1200,1201. 把 4,3,5 分别乘以 $2\cdot 5\cdot(4^2-3^2)=70$,"放大"后的三角形成为 280,210,350. 而这两个三角形的面积都等于 29400.

三个本原毕氏三角形所共有的最小面积是 13123110. 这三个三角形的边长分别是:4485,5852,7373;19019,1380,19069;3059,8580,9109. 它们各自对应于其母数:77,38;138,5;78,55.

具有相等面积的三个毕氏三角形也可从算术级数的相连四项中产生出来. 设 a, b, c, d 为这四项,则母数 $m=ab, n=cd$ 能得出第一个三角形;母数 $a(c-b), c(c+b)$ 可得出第二个三角形;母数 $d(c-b), b(c+b)$ 可得出第三个三角形. 若令 a, b, c, d

分别取 1,2,3,4 的值，则上述母数将是 2,12;1,15;4,10;与之对应的三个三角形，其直角边是 140,48;224,30;84,80，而它们中的每一个，其面积都等于 3360.

下面是四个等积的毕氏三角形的为数甚少的几例. 字母 m，n 是三角形的母数，而两直角边之边长为 $k(m^2-n^2)$ 与 $k(2mn)$.

	1			2			3			4		
面积	m	n	k	m	n	k	m	n	k	m	n	k
341880	56	55	1	40	37	1	37	7	1	37	33	1
17957940	92	77	1	165	4	1	23	12	13	28	5	13
116396280	133	88	1	152	35	1	153	133	1	133	65	1
1071572040	232	155	1	301	40	1	301	279	1	319	301	1
1728483120	259	144	1	368	35	1	259	155	1	299	259	1

问题 9 与问题 10 留给读者去求解.†

*　　　*　　　*

下面的问题原先出现于《美国数学月刊》:"试求某种图式，以使得人们能机械地写出一系列正整数边长的直角三角形而不需任何计算."此问题的解法如下：在关系式 $a^2+b^2=c^2$ 中，设 $c=b+1$，于是 $a^2=c^2-b^2=b^2+2b+1-b^2=2b+1$，由于 a^2 是个奇数，所以 a 也应该是奇数，设它等于 $2n+1$，于是 $a^2=4n^2+4n+1$，$b=(a^2-1)/2=2n^2+2n$. 从而 $c=b+1=2n^2+2n+1$. 若把 n 选为 10 的正整数幂，则我们就可以造出一张表格，开头的三个数是 21,220,221，以后在中间不断插入 0，如表 61 所示. [127]

n	$a=2n+1$	$b=2n^2+2n$	$c=2n^2+2n+1$
10	21	220	221
10^2	201	20200	20201
10^3	2001	2002000	2002001
10^4	20001	200020000	200020001
10^5	200001	20000200000	20000200001
10^6	2000001	2000002000000	2000002000001

表 61　可以机械地写出来的毕氏三角形

类似地,也可从 $n=20$ 开始,即 10 的正整数次幂的二倍,由

$$41^2+840^2=841^2,$$

接下去的是

$$401^2+80400^2=80401^2,$$

等等.

也可以从 $a=6n+9, b=2n^2+6n, c=2n^2+6n+9$ 开始,则当 n 为 10 的正整数次幂时,有一连串等式:

$$69^2+260^2=269^2,$$
$$609^2+20600^2=20609^2,$$

等等,依此类推.

* * *

1643 年,费马写信给梅桑,要求找出一个毕氏三角形,其两直角边之和以及斜边均为平方数. 若三边记为 X, Y, Z,那就意味着要求如下关系式解成立:

$$X+Y=a^2,$$
$$Z=b^2, \tag{1}$$
$$X^2+Y^2=Z^2=b^4.$$

其解法显示了费马的著名方法"无限递降法"的一个实例,但这里并不是证明条件不可能,而是表明怎样从某种形式的方程的最少可能的解开始,一步步地得出其他解答,直至题目条件得到满足为止. 这种办法是非常巧妙的. [128]

设

$$X-Y=e. \tag{2}$$

把(1)式与(2)式联立起来,解出 X 与 Y,得到

$$X=(a^2+e)/2, \quad Y=(a^2-e)/2,$$

则

$$X^2+Y^2=(2a^4+2e^2)/4=(a^4+e^2)/2=Z^2=b^4,$$

即

$$a^4+e^2=2b^4 \quad 或 \quad 2b^4-a^4=e^2. \tag{3}$$

由基本的毕氏三角形公式，我们有：$X=m^2-n^2$；$Y=2mn$；$Z=m^2+n^2=b^2$. 但最后一个 Z 的表达式本身便是一种毕氏三角形关系，故而有：

$$m=r^2-s^2; \quad n=2rs; \quad b=r^2+s^2. \tag{4}$$

由（1）式，$m^2-n^2+2mn=a^2=(m+n)^2-2n^2$ 或 $(m+n)^2-a^2=2n^2$，也就是说，我们必须求出两个平方数，它们的差是某个平方数的二倍. 但 $A^2-B^2=2C^2$ 的通解为：$A=t^2+2u^2$；$B=t^2-2u^2$；$C=2tu$，这是极容易验证的. 在此例中我们有 $A=(m+n)$；$B=a$；$C=n$，于是 $m+n=t^2+2u^2$，$n=2tu$，从而有 $m=t^2+2u^2-2tu$. 用 t 与 u 表达的 m,n 同(4)式中用 r 与 s 表达的 m,n 当然应该相等，于是有：

$$\begin{aligned} r^2-s^2&=t^2+2u^2-2tu, \\ 2rs&=2tu. \end{aligned} \tag{5}$$

要求这些参变量的正整数值以同时满足两个方程. 由 $rs=tu$ 可得 $r/t=u/s$. 假定这两个分数的最简分数是 d/c. 于是 $r=kd$；$u=Ld$；$t=kc$；$s=Lc$. 代入(5)并合并整理，即得：

$$L^2(c^2+2d^2)-2cdLK+k^2(c^2-d^2)=0,$$

除以 k^2 后，得

$$(L/k)^2(c^2+2d^2)-2cd(L/k)+(c^2-d^2)=0.$$

用一元二次方程求根公式解出 L/k，便得

$$L/k=[cd\pm(2d^4-c^4)^{\frac{1}{2}}]/(c^2+2d^2).$$

这就要求 $2d^4-c^4$ 应是一个平方数，设它是 V^2，于是有

[129]

$$2d^4-c^4=V^2. \tag{6}$$

现在可以看到：(6)式的形状简直同(3)式完全一样，仅不过涉及的数字要较小一些. 于是我们又可从(6)式开始，通过类似的解析步骤而再次得到一个与它类似而数值更小的关系式. 由此可见，如果真的有解，则最小的解必然会达到的. 而这个最小解是 $2\cdot1^4-1^4=1^2$. 这里 $d=c=V=1$，从这些数量回溯，可以得到(3)中的 b,a,e. 如果我们为 X,Y,Z 所定下的条件得到满足，那么解便找到了；如果还不满足，那么我们就令 $b=d_1,a=c_1,e=V_1$，再照葫芦画瓢地进行下去来求得新的 b,a,e 值，直至最后求出所需要的解为止.

在代入数值之前，让我们略为总结一下上述步骤：

(1) V,c,d 是满足方程 $2d^4-c^2=V^2$ 的任何正整数，例如 1,1,1.

(2) $L=cd\pm V$,
$k=c^2+2d^2$,
$r=kd$,
$s=Lc$.

(3) $m=r^2-s^2$,
$n=2rs$,
$b=r^2+s^2$.

(4) $X=m^2-n^2$,
$Y=2mn$,
$Z=b^2$.

(5) $X+Y=a^2$,
$X-Y=e$.

先假定 $d=c=V=1$，便可得到

$$L/k=(1\pm1)/3=0/3 \text{ 或 } 2/3.$$

$L=0$ 这个值自应丢弃；在 $L=2,k=3$ 时将有 $r=kd=3,s=Lc=2$；$m=5,n=12$；$X=-119,Y=120,Z=169=13^2$. 不幸的是，作为毕氏三角形的一边，-119 这个值是不能接受的. 连续进行下去，求 b,a,e 的值，此时即有 $r^2+s^2=b=13$；$X+Y=a=$

$1, X-Y=e=-239$. 方程(3)与(6)可得到满足，即 $2\cdot 13^4-1^4=(-239)^2$.

让我们再一次重新来过，$d_1=13; c_1=1; V_1=-239$. 则有 $L/k=(13\cdot 1\pm 239)/(1+2\cdot 13^2)=252/339=84/113$ 或 $(-226)/339=-2/3$. 取 $L=-2, k=3$；则 $r=39, s=-2$，而 $m=r^2-s^2=1517, n=-156; X=2276953, Y=-473304$. 由于 Y 的值是负数，我们只好再次舍弃，改为再试 $L=84, k=113$. 于是 $r=1469, s=84; m=2150905, n=246792$;

$$X=m^2-n^2=4565486027761,$$
$$Y=2mn=1061652293520,$$
$$Z=b^2=4687298610289=2165017^2.$$

[130]

并且

$$X+Y=a^2=2372159^2=5627138321281.$$

看来很难相信这三个数是满足给定条件的最小数，但真相确是如此. 正如人们所猜想的那样，第二个最小解所得出的数目，如果表示成英尺或英寸数，由此而形成的毕氏三角形的两条直角边，无疑将会超出银河系的边界.

* * *

毕氏三角形的周长等于

$$K(m^2-n^2)+K(2mn)+K(m^2+n^2)=K(2m^2+2mn)$$
$$=2Km(m+n).$$

要想求出周长相等的毕氏三角形，实际上意味着怎样将一个数用多种方法表示成 $2Km(m+n)$ 的形式. 此事看来非常容易，但事实上这些数字并不很小，找起来也不太容易. 下面的表格中给出了五组实例，每组有三个本原毕氏三角形，周长都一样，母数 m, n 以及周长 p 也都给出：

周长	1		2		3	
$p=2m(m+n)$	m	n	m	n	m	n
14280	60	59	68	37	84	1
72930	187	8	165	56	143	112
81510	195	14	165	82	143	142
92820	170	103	182	73	210	11
103740	182	103	190	83	210	37

这五例中的三角形都是本原的，但如果允许用非本原三角形，则三数组中可以有为数很小的周长，例如 120. 这样的三个直角三角形，其边长分别为(20，48，52)，(45，24，51)，(40，30，50).

*　　*　　*

有相同周长的四个本原毕氏三角形也已经发现. 对周长小于 1，000，000 的四个三角形组，只有七个实例，因而可以说是相[131]当稀少的. 这些周长中，最小者为 317460；对应的母数是(286，269)，(330，151)，(370，59)，(390，17)；四个三角形的边长分别是(153868，9435，154157)，(99660，86099，131701)，(43660，133419，140381)，(13260，151811，152389). 读者们能找出另外六个解吗？†

*　　*　　*

边长为 693；1924 与 2045 的本原毕氏三角形，其面积为 666666.①

*　　*　　*

有许多毕氏三角形，它们的面积数用遍了 9 或 10 个不同数码. 由母数 149 与 58 所产生的毕氏三角形，其面积为 162789354；用母数 224 与 153，所得之面积为 917358624. 母数 666 与 5 能产生面积 1476958230；母数 406 与 279 产生面积

① 读者们也许会感到奇怪，为什么要特别举出 666666 呢？原来，666 是《圣经》里的野兽数，西方人对它特别忌讳. ——译者注.

9854271630，则十个数码都齐备了.

*　　*　　*

任一对毕氏三角形都以一种奇妙方式相互联系.若 $A,B,C;a,b,c$ 分别表示两个直角三角形的直角边与斜边，则必有 $(C+c)^2-(A+a)^2-(B+b)^2=D^2$，结果为一平方数.进一步还有以下关系式：

$$Cc-Aa-Bb=2E^2,\ Cc-Ab-aB=J^2,$$
$$Cc+Aa+Bb=2F^2,\ Cc+Ab+aB=K^2,$$
$$Cc-Aa+Bb=2G^2,\ Cc+Ab-aB=L^2,$$
$$Cc+Aa-Bb=2H^2,\ Cc-Ab+aB=M^2.$$

*　　*　　*

任意复数的平方可得出毕氏三角边的两直角边.例如 $(2+i)^2=3+4i$，而 $3^2+4^2=5^2$.另外还有

$$(3+2i)^2=5+12i，而\ 5^2+12^2=13^2.$$

一般地说，

$$(a+bi)^2=(a^2-b^2)+2abi，而(a^2-b^2)^2+(2ab)^2=(a^2+b^2)^2.$$

读者们当能回忆得起 $i=\sqrt{-1},i^2=-1,i^3=-i,i^4=+1$.

通过这种办法，可以求得和为 n 次幂的两个平方数.例如可取 $a=2,b=1$，则有

$$(2+i)^3=8+12i+6i^2+i^3=2+11i\ 而\ 2^2+11^2=5^3.$$ [132]

再来看 $(3+2i)^4=81+216i+216i^2+96i^3+16i^4=-119-120i$，此时可得关系式 $119^2+120^2=13^4$.一般地说，利用二项式定理来展开 $(a+bi)^n$，使 x,y 分别取实部与虚部的系数，即可获得 $x^2+y^2=z^n$ 的关系.若 z 之值能分拆为 a^2+b^2，则对任意正整数 n，都易于找到 $x^2+y^2=z^n$ 的关系.例如，$z=13=3^2+2^2$，而 $n=3$，则通过 $(3+2i)^3$ 的展开，可以找到两个平方数，而其和是等于

$13^3=2197$的.实部和虚部的系数即为所求的数x,y,对本例来说就是9与46,从而得到关系式$9^2+46^2=13^3$.

参考文献

Anema, A. S. "Pythagorean Triangles with Equal Perimeters," *Scripta Mathematica*, **15**(1949), 89.

Barlow, P. *Theory of Numbers*. London: J. Johnson & Co., 1811.

Block, D., and Umansky, H. L. "Pythagorean Variations," *Scripta Mathematica*, **15**(1949), 244.

Carmichael, R. D. *Theory of Numbers and Diophantine Analysis*. New York: Dover Publications, Inc., 1959.

Cheney, W. F., and Rosenbaum, J. "Solution to Problem: Show That There Is Just One Right-Triangle Whose Three Sides Are Relatively Prime Integers Between 2000 and 3000," *American Mathematical Monthly*, **41**(1934), 393.

Christie, R. W. D. "Problem: Prove That $(\Sigma p_n)^2+(\Sigma p_n+1)^2=(p_{2n}+q_{2n})^2=q_{2n+1}^2$ Where Σp_n Signifies the Sum of the Even Convergents of $p^2-2q^2=\pm 1$," *Mathematical Gazette*, **1**(1896—1900), 394.

Dickson, L. E. *History of the Theory of Numbers*. 3 vols. New York: Chelsea Publishing Co., 1950.

——. *Introduction to the Theory of Numbers*. New York: Dover Publications, Inc., 1957.

Ginsburg, J. "Complex Numbers as Generators of Pythagorean Triangles," *Scripta Mathematica*, **13**(1947), 105.

——. "Triplets of Equiareal Rational Triangles," *Scripta Mathematica*, **20**(1954), 219.

Gruber, M. A., *et al.* "Solution to Problem: Find the First

Six Sets of Values in Which the Sum of Two Consecutive Integral Squares Is a Square," *American Mathematical Monthly*, **4**(1897), 24.

Hopkins, G. H. "Solution to Problem: [Find Two Consecutive Integral Squares Whose Sum Is a Square]," *Mathematical Questions from the Educational Times*, **12**(1869), 104.

Licks, H. E. *Recreations in Mathematics*. New York: D. Van Nostrand, 1921.

[133]

Loyd, S. *Cyclopedia of Puzzles*. New York: Lamb Publishing Co., 1914.

——. *Mathematical Puzzles of Sam Loyd*, ed. by Martin Gardner. 2 vols. New York: Dover Publications, Inc., 1959—1960.

Martin, A. "Solution to Problem: [Find Two Consecutive Integral Squares Whose Sum Is a Square]," *Mathematical Questions from the Educational Times*, **14**(1871), 89.

——. "Solution to Problem: [Find Two Consecutive Integral Squares Whose Sum Is a Square]," *Mathematical Questions from the Educational Times*, **16**(1872), 107.

——. "Solution to Problem: [Find Two Consecutive Integral Squares Whose Sum Is a Square and Find the Eightieth Such Set]," *Mathematical Questions from the Educational Times*, **20**(1874), 42.

——. "Rational Right-Triangles Nearly Isosceles," *The Analyst*, **3**(1876), 47.

——. "Solution to Problem: [Integral Right-Triangles Whose Legs Differ by Unity]," *Mathematical Visitor*, **1**(1879), 55.

Miksa, F. L. "Pythagorean Triangles with Equal Perimeters," *Mathematics*, **24**(1950), 52.

——. "Table of Primitive Pythagorean Triangles Whose Areas Contain All (10) Digits," *Scripta Mathematica*, **20**(1954), 231.

Moessner, A. "If—Then," *Scripta Mathematica*, **18**(1950), 164.

Ozanam, J. *Recreations in Science and Natural Philosophy*. London: T. Tegg, 1884.

Putnam, K. S. "Solution to the Problem: [Pythagorean Triangles Whose Legs Differ by Unity]," *Mathematical Visitor*, **1**(1879), 122.

Shedd, C. L. "Another Triplet of Equiareal Triangles," *Scripta Mathematica*, **11**(1945), 273.

——. "Equiareal Triangles," *Scripta Mathematica*, **16** (1950), 293.

Uspensky, J. V., and Heaslet, M. A. *Elementary Number Theory*. New York: McGraw-Hill Book Co., 1939.

Vinogradov, I. M. *Elements of Number Theory*. New York: Dover Publications, Inc., 1954.

Whitlock, W. P., Jr. "An 'Impossible' Triangle," *Scripta Mathematica*, **9**(1943), 189.

Wilkinson, T. T. "Problem: [Rule for Finding Integral Right-Triangles Whose Legs Differ by a Given Number]," *Mathematical Questions from the Educational Times*, **20** (1874), 20.

Willey, M., and Kennedy, E. C. "Solution to Problem: [Find a Scheme for Writing Mechanically an Unlimited Number of Pythagorean Triangles]," *American Mathematical Monthly*, **41**(1934), 330.

第15章 平方奇观

请想一想，正方形可有意思哩：它多么完美，多么对称．所有的边都相等，每只角既非笨得迟钝，又非险得尖锐，它们不锐不钝，正好是直角．正方形有许多美妙的几何性质．读者们或许能回忆得起，怎样通过圆规、直尺作图法把任一矩形转化成正方形．方法是先找到矩形两条邻边的“比例中项”．此外，还有大名鼎鼎的毕达哥拉斯定理：“直角三角形两条直角边上的正方形面积之和等于斜边上的正方形面积．”

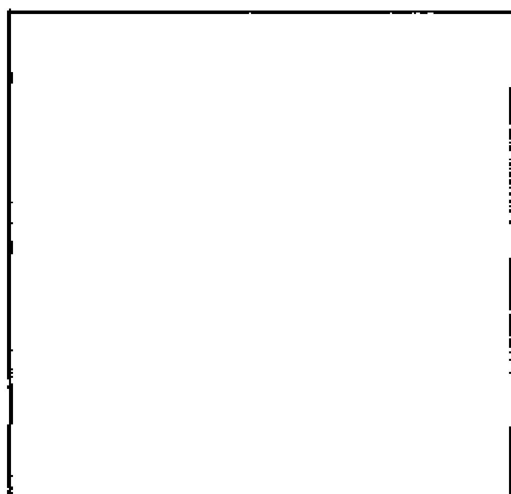


图 7 一个正方形

这里我们不想多谈正方形的几何性质，而主要从数值角度来考察这种正四边形．所谓平方数是数列 1，4，9，16，25，…中的整数．在数列的连续两项之间不难看到一种关系，那便是，第一

个平方数加上3，就能得出第二个平方数，而后者再加上5，又可得出第三个平方数，如此等等。一般地说，如果把$2x+1$加到x的平方上去，即可得出下一个平方数，即：$x^2+(2x+1)=(x+1)^2$。例如$5^2+2\cdot5+1=6^2$。
[135]

已知一个平方数，下一个平方数立即可以写出。例如，若已知$18^2=324$，则下一个平方数是

$$19^2 = 18^2 + 2\cdot18 + 1 = 324 + 36 + 1 = 361.$$

以5为尾数的数的平方可以脱口而出，拿35的平方来说，把首位的3乘上比它大1的连续数4，在其后面添加尾巴25，结果1225就出来了。用此办法不难马上算出$65^2=4225$($6\times7=42$，后面再加上“尾巴数”25)，$15^2=225$等等，二位以上的数求平方时，也可如法炮制，例如$115^2=13225$。

*　　　*　　　*

根据人们非常熟悉的代数恒等式

$$(a+b)^2 = a^2 + 2ab + b^2,$$

以及

$$(a-b)^2 = a^2 - 2ab + b^2,$$

其特例自然是

$$(a+1)^2 = a^2 + 2a + 1,$$

与

$$(a-1)^2 = a^2 - 2a + 1.$$

于是，若已知$60^2=3600$，用心算作加法即可算出

$$61^2=(60+1)^2=60^2+2\cdot60+1=3600+120+1=3721,$$

类似地有

$$59^2=(60-1)^2=60^2-120+1=3600-120+1=3481.$$

稍为困难一些的是

$$(a \pm 2)^2 = a^2 \pm 4a + 4.$$

此时即有

$$62^2 = (60 + 2)^2 = 3600 + 4 \cdot 60 + 4 = 3844,$$
$$58^2 = (60 - 2)^2 = 3600 - 4 \cdot 60 + 4 = 3364.$$

* * *

末位数为 0 的数，其平方当然很容易，末位为 5 的数的平方，上面已经讲过了. 与原数相差 1 或 2 的数，其平方也有简捷办法. 这些东西加在一起，就几乎把平方数的空隙覆盖得差不多. 例如，70 与 80 之间的平方数，我们几乎都能马上写出来，计算量很少： [136]

$70^2=4900$,

$71^2=(70+1)^2=70^2+2 \cdot 70+1=5041$,

$72^2=(70+2)^2=70^2+4 \cdot 70+4=5184$,

$73^2=(75-2)^2=75^2-4 \cdot 75+4=5625-300+4=5329$,

$74^2=(75-1)^2=75^2-2 \cdot 75+1=5625-150+1=5476$,

$75^2=5625$（在 $7 \times 8=56$ 的后面添写 25），

$76^2=(75+1)^2=75^2+2 \cdot 75+1=5625+150+1=5776$,

$77^2=(75+2)^2=75^2+4 \cdot 75+4=5625+300+4=5929$,

$78^2=(80-2)^2=80^2-4 \cdot 80+4=6400-320+4=6084$,

$79^2=(80-1)^2=80^2-2 \cdot 80+1=6400-160+1=6241$,

$80^2=6400$，等等.

稍加练习，即可背熟 1 到 100 的平方数. 这是治疗失眠症的一帖良药.

另一个甚至更为简易的办法是利用熟知的代数公式：

$$(a + b)(a - b) = a^2 - b^2.$$

移项后得

$$(a + b)(a - b) + b^2 = a^2.$$

设待求的是a^2，于是可以适当地选取b，以使$a+b$或$a-b$为简易乘数（譬如其末位数为0）. 例如

$$47^2=(47+3)(47-3)+3^2=50\cdot 44+9=2209,$$

$$96^2=(96+4)(96-4)+4^2=100\cdot 92+16=9216,$$

$$\begin{aligned}113^2&=(113+13)(113-13)+13^2\\&=126\cdot 100+169=12769\\&=(113+3)(113-3)+3^2\\&=116\cdot 110+9=12769,\end{aligned}$$

$$\begin{aligned}179^2&=(179+21)(179-21)+21^2\\&=200\cdot 158+441=32041.\end{aligned}$$

* * *

对某些自然数区间，存在着非常快速有效的心算法以获取平方数. 例如40至60间的平方数，计算时可用25加上超过50的“过剩数”或不足50的“亏损数”，并在此结果的后面添上过剩数或亏损数的平方. 例如，对54^2而言，过剩数是4，加上25后得出29，再在后面添写4的平方16，于是马上得出2916，即54的平方. 类似地再来看57的平方，此时有$25+7=32$，而$7^2=49$，于是$57^2=3249$. 若过剩数的平方只有一位数，则要在前面添个0，以凑足二位，例如在算53^2时，$25+3$后面再添写09，便得$53^2=2809$. 对46^2来说，亏损数是4，于是在$25-4$的后面添写4^2，即得$46^2=2116$，对48^2则有$25-2$再添写04，结果是$48^2=2304$.

[137]

这种简捷办法据云来自伦赛勒综合工艺学院的詹姆士·麦克吉弗特(James McGiffert)教授. 方法之所以能成立，理由很明显. 这是由于

$$(50\pm x)^2=2500\pm 100x+x^2=(25\pm x)100+x^2.$$

用100乘上$(25\pm x)$意味着在积的十位与个位数留出空位，正好给表示为二位数的x^2来填补. 此公式中并没有排斥x大于

10 的情况，但其时 x^2 将不止二位，操作起来就不方便了. 例如对 63^2 来说，将有 $25+13$，再添写 13^2，即得 38 与 169，也就是 3969. 或在计算 36^2 时有 $25-14$，再添写 14^2，即 11 与 196，亦即 1296.

在计算 20 到 29 的平方时也可置于适合使用上述规则的数的区间，只要记住某数的平方是此数二倍再平方的四分之一. 例如要计算 28^2，可先用上述法则计算 56^2，再将结果除以 4. 类似地，计算 82 至 98 之间偶数的平方时，可先除以 2，再应用上述规则，最后再乘上 4. 例如在算 82^2 时，我们可先算 41^2，在 $25-9$ 的后面添写 $9^2=81$，得 1681 后，再乘以 4，结果便是 6724.

对 90 至 110 之间的数也有一个类似规则.

$$(110\pm x)^2=10000\pm 200x+x^2=(100\pm 2x)100+x^2$$
$$=(100\pm x\pm x)100+x^2.$$

当然它也可用于计算一切整数的平方，但对 90 到 110 之间的平方数更为方便. 例如在计算 104^2 时我们将有 $104+04$ 并在后面添写 16，即得 10816，类似地算 109^2 时有 $109+09$，再添写 81，故得 11881. 此外还有 97^2，先写 $97-3=94$，再在后面添上 3^2，最后便是 9409，以及 $94^2=8836$ 等等.

还有许多简便规则可用，但大多数人，也包括本书作者在内，学会以后不久就马上忘记了.

*　　　*　　　*

彼得・巴罗(Peter Barlow)曾印刷出版过一张从 1 至 10000 的平方数表. 对数论爱好者来说，此表极为有用，也很容易搞到它的现代版. 巴罗的原始版本完工于 1814 年 7 月 1 日. [138] 但是，甚至早在 1781 年，直到 25400 为止的平方数表在一个名叫休顿博士(Dr. Hutton)手中即已公开刊行.

仔细察看一下这类表格，就会发现平方数的某些有趣性质. 譬如说，它们全都以 0，1，4，5，6，9 结尾，决不会是 2，3，7，8. 用

数论说法来讲，前一组数字中的每一个是 10 的平方剩余，而后一组数字中的每一个却是平方非剩余. 这下子人们有了简单的目测法，尽管这不过是判别平方数的必要条件，不是充分条件. 以 0，1，4，5，6，9 结尾的数未必就是平方数，但不是以这些数结尾的数则肯定不是平方数.

一个更好的排他性测试是检查最后二位尾数，即“100 的平方剩余”. 它们一共有 22 个，大于 9 的平方数，其最后二位尾数肯定是表 62 中列举的尾数之一.

00	21	41	64	89
01	24	44	69	96
04	25	49	76	
09	29	56	81	
16	36	61	84	

表 62　二位平方尾数

在研究数的某些形式时，它是极其有用的信息. 我们经常想确定一个数在加上或减去一平方数以后，其和或差是否为平方数. 上述二位尾数就能帮助我们迅速排除那些不可能的情况. 例如我们要求一个平方数 x^2，使 $5581-x^2$ 是平方数，表格就会告诉我们，x^2 的结尾只能是 00，25，56 或 81.（答案应为 $x^2=4356=66^2$，而 $5581-4356=1225=35^2$.）

二位尾数 00 与 44 是具有相同数码的唯一结尾. 平方数自然可能以任意偶数个零来结尾，但是，任何平方数尾部都不可能具有三个以上的 4，而 $38^2=1444$ 是这类数字中的最小者. 它与下一个数 $462^2=213444$ 中间空出一大段. 在此之后，则是 $538^2=289444$ 与 $962^2=925444$. 一般地说，$500x\pm38$ 是平方后结尾有三个 4 的数. 此处，x 可为任意整数，也包括 0 在内.

[139]　　* * *

本书的许多读者无疑已经熟知上文所述的平方数的末位尾数法则，但未必知道平方数应该满足的另一条件. 除非一个数的

各位数字之和等于 1,4,7,9,它不可能是一个平方数.此性质可证明如下:一切整数用 9 去除时必然留下余数 0,1,2,3,4,5,6,7,8;也就是说,一切整数均可表示为如下形式:$9a$,$9a\pm1$,$9a\pm2$,$9a\pm3$,$9a\pm4$.这些数目的平方除以 9 时,其余数必为 0,1,4,9,7.但是,前已说过,一个数用 9 除时留下的余数与该数的各位数码之和被 9 去除时留下的余数是相同的(见第 8 章),这样就证明了上述法则.余数 0 实际上就是余数 9;显然一个数的各位数码之和不可能等于 0,除非该数本身为 0.

*　　*　　*

平方数及其性质一直深深地吸引住数学家,因此总是有人试图把一切关系转化为平方关系.任意大于 1 的奇数,从 8 开始的 4 的倍数都能至少用一种办法表示为两个平方数之差.但是,奇数的二倍是不能表示为两个整数的平方差的.给定 A 时,要想解方程 $x^2-y^2=A$,可令 $x+y$ 等于 A 的任一除数(但应大于 A 的平方根),再令 $x-y$ 等于相补的除数.这两个除数必须同为偶数或同为奇数,即奇偶性必须相同,然后再从 $x+y$ 与 $x-y$ 的联立方程中解出 x 与 y.

*　　*　　*

第 14 章已讲过,作为毕达哥拉斯三角形斜边 H 的整数所应满足的条件:$H=K(m^2+n^2)$.它实际上等价于 $2^{a_0}QP$,这里 a_0 是包括 0 在内的任意整数,Q 为形为 $4x-1$ 的素数的乘幂之积,而 P 为 $4x+1$ 形式的素数的乘幂之积.如果至少有一个 $4x+1$ 形式的素数,则 P 恒能表示为两个整数的平方和 m^2+n^2;再令 K 等于 $2^{a_0}Q$,我们便得到了 H 的所需形式(实际上 K 可为任意整数).与此有联系的问题是要找出一个整数可表示为两个整数平方和的条件.为了满足此项要求,Q 必须代之以 Q^2,因而若一整数可表示为两个整数平方和,则它必取 $2^{a_0}Q^2P$ 的形状(此时 [140] $K=2^{a_0}Q^2$ 或者是一个平方数,或者是平方数的二倍,而不仅仅是一个整数,这是一个比以前更为苛刻的限制).作为一个实例,

$2^7 \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 13^3$ 可以记为 $2^7(3^2 \cdot 7)^2(5 \cdot 13^3)$，后者符合所需的形式.本章的后面部分将作出交代，怎样才能把此数表示为两个平方数之和.

表示为 $N=2^{a_0}p_1^{2a_1}p_2^{2a_2}\cdots p_n^{2a_n}q_1^{b_1}q_2^{b_2}\cdots q_r^{b_r}$ 形式的数（此处 p 为 $4x-1$ 形式的素数，q 为 $4x+1$ 形式的素数）是

$$[(2b_1+1)(2b_2+1)\cdots(2b_r+1)-1]/2$$

个毕氏三角形的斜边；但只是两个非零的、不相等的平方数之和，此种表示法当分子为偶数时共有

$$(b_1+1)(b_2+1)\cdots(b_r+1)/2 \qquad \text{（公式 1）}$$

种；而当分子为奇数时，则有

$$[(b_1+1)(b_2+1)\cdots(b_r+1)/2]-1/2 \qquad \text{（公式 2）}$$

种.例如，$N=2^7 \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 13^3$ 可视为

$$[(2\cdot 1+1)(2\cdot 3+1)-1]/2=10$$

个毕氏三角形的斜边；但只有

$$(1+1)(3+1)/2=4$$

种办法把它表示为两个平方数之和.只有素数 5 与 13 的指数要利用，而其他的素数则不予考虑.

这里要解释一下上文所提到的定语“不相等的平方数”.任何一个平方数的二倍 $2x^2$ 可记为 x^2+x^2，这也是两个平方数之和.如果相等的平方数也可允许的话，则由公式 2 给出的解数要增加一个，或者在无解的情况下将它看作一个解.（这里要用公式 2 而不是公式 1，因对 $2x^2$ 而言，它的一切奇素数因子的指数必为偶数，此类指数的乘积加 1 以后必为奇数，可见分子是奇数，这就要求使用公式 2.）因此，对 $2 \cdot 5^2 \cdot 13^2$ 来说，公式 2 表明它有

$$[(2+1)(2+1)/2]-1/2=4$$

个解，但 $5^2 \cdot 13^2+5^2 \cdot 13^2$ 可看作是第五解. 另外，对 $2 \cdot 3^2=18$ 来说，按公式 2，它应视为无解，因为数 18 是不含有 $4x+1$ 形式的除数的. 但按照上面的说法，也可看作它有 3^2+3^2 这个解. [141]

对平方数的二倍作了这种补充说明之后，于是公式可以修改为

$$(b_1+1)(b_2+1)\cdots(b_n+1)/2-[(-1)^{a_0}]/2.$$

当 2 的指数 a_0 为奇数时，N 是平方数的二倍，公式 2 中的 $-\frac{1}{2}$ 将变作 $+\frac{1}{2}$，从而添加一解；当 a_0 为偶数时，原先的数 N 不可能是平方数的二倍，于是 $-\frac{1}{2}$ 保持不变，从而不增加新解.

雅可比给出了一个巧妙规则来说明一个数表示为两个平方数之和时究竟有多少种方法：把 $4x+1$ 形式的除数超过 $4x-1$ 形式的除数的个数再乘上 4. 但须注意在此规则中：(1) 把 0 也看成一个平方数；(2) 平方数看成是正数与负数的平方；(3) 两个平方数的先后次序也要考虑，因此 $(\pm 3)^2+(\pm 4)^2$ 将视为八解. 所以公式 1 与公式 2 较为合适，也符合一般人对于"两平方数之和"的理解.

第 14 章已提到过一桩神奇性质，每个形如 $4x+1$ 的素数都能唯一地表示为两个互质数的平方和. 这种唯一表示法对此种素数的乘幂以及乘幂的二倍也是成立的. 具体例子有：$5=1^2+2^2$；$2 \cdot 5=1^2+3^2$；$5^3=2^2+11^2$；$2 \cdot 5^3=9^2+13^2$. 但是，对于 $4x-1$ 形式的数，不论它是素数或合数，均不能表示为两个平方数之和.

上述公式 1 或公式 2 也能表示单个 $4x+1$ 形式的素数乘幂表为两平方数之和的方法数. 我们可按乘幂的或奇或偶交替地使用这两个公式. 如选取此类素数的最小者 5，我们即可得出表 63.

N^n	把 N^n 表示为两平方数之和的方法数		解
	任何方式	互质的方式	
5	1	1	**1^2+2^2**
5^2	1	1	**3^2+4^2**
5^3	2	1	5^2+10^2; **2^2+11^2**
5^4	2	1	15^2+20^2; **7^2+24^2**
5^5	3	1	25^2+50^2; 10^2+55^2; **38^2+41^2**
5^6	3	1	75^2+100^2; 35^2+120^2; **44^2+117^2**
5^7	4	1	50^2+275^2; 125^2+250^2; 190^2+205^2; **29^2+278^2**
5^8	4	1	175^2+600^2; 375^2+500^2; 220^2+585^2; **336^2+527^2**
5^9	5	1	250^2+1375^2; 950^2+1025^2; 625^2+1250^2; 145^2+1390^2; **718^2+1199^2**
5^{10}	5	1	875^2+3000^2; 1875^2+2500^2; 1100^2+2925^2; 1680^2+2635^2; **237^2+3116^2**

[142] **表 63 素数 $N=4x+1=5$ 的乘幂表示为两平方数之和**

值得注意的是，在互质情况下只有一种表示法，表中用粗体字排出. 这对素数、素数的方幂以及此等数字的二倍都是如此.

*　　　*　　　*

两个平方数之和乘以两个平方数之和，所得之乘积仍是两个平方数之和. 这种关系真是奇妙！由 $5=2^2+1^2$，$13=3^2+2^2$，我们得出 $5\cdot 13=65=8^2+1^2$ 或 7^2+4^2. 这种关系来自代数恒等式：

$$(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2$$
$$=(ac-bd)^2+(ad+bc)^2. \qquad \text{(公式 3)}$$

如果原来的乘积中两个因子完全一样，则有：

$$(a^2+b^2)(a^2+b^2)=(a^2+b^2)^2=(a^2-b^2)^2+(2ab)^2,$$
（公式 4）

此时仍可视为两个平方数之和，但表达法只有一种. 例如，

$$(3^2+2^2)(3^2+2^2)=13^2=(3^2-2^2)^2+(2\cdot 3\cdot 2)^2$$
$$=5^2+12^2.$$

请注意，公式 4 是一种毕氏三角形的关系，犹如第 14 章中的公式 1.

如在公式 3 的原来乘积中，令 $c=d=1$，则有

$$2(a^2+b^2)=(a+b)^2+(a-b)^2,\qquad（公式 5）$$ [143]

它仍可视为两个平方数之和，但只有一种表示法. 例如：

$$2(3^2+1^2)=(3+1)^2+(3-1)^2=20.$$

两平方数之和也可以是一立方数. 由公式 4，$(a^2+b^2)^2=(a^2-b^2)^2+(2ab)^2$，两端同乘以$(a^2+b^2)$，并利用公式 3，即有

$$(a^2+b^2)^3=[(a^2-b^2)^2+(2ab)^2](a^2+b^2)$$
$$=(a^3+ab^2)^2+(-a^2b-b^3)^2,$$

也可变换到

$$(a^3-3ab^2)^2+(3a^2b-b^3)^2.$$

令 $a=2$，$b=1$ 并代入上两式，即得 $10^2+5^2=5^3$，$2^2+11^2=5^3$. 可见(a^3+ab^2)与$(-a^2b-b^3)$各自平方之和或(a^3-3b^2)与$(3a^2b-b^3)$各自平方之和都是立方数. 采用类似办法可以导出两平方和等于 n 次方的公式.

*　　　*　　　*

现在我们准备讲一讲怎样才能完成一桩令人生畏的任务，把数 $2^7\cdot 3^4\cdot 5\cdot 7^2\cdot 13^3$ 表示为两平方数之和. 显然，5 与 13 是 $4x+1$ 形状的素数，因而我们已经知道它们中的每一个都可表

示为两个平方数之和.但当素数很大时，要做到这一点相当不容易.艾伦·克宁汉在其编造的庞大表格“平方分割”中给出了此种办法，表中给出的 $4x+1$ 形状的素数是不超过100,000的.但对5与13这种很小的素数来说，根本不必去查表，一眼即可看出 $5=2^2+1^2$，$13=3^2+2^2$.由公式3：

$$5\cdot 13=(2^2+1^2)(3^2+2^2)=(6+2)^2+(4-3)^2 \\ =8^2+1^2,$$

或也可表示为

$$(6-2)^2+(4+3)^2=4^2+7^2.$$

它们叫做第1解与第2解.现在让我们改写原数，把具有偶指数的乘幂集于一组，这样一来就把 $2^7\cdot 3^4\cdot 5\cdot 7^2\cdot 13^3$ 改记为 $(2^6\cdot 3^4\cdot 7^2\cdot 13^2)(2\cdot 5\cdot 13)$.利用公式5我们可将 $2\cdot 5\cdot 13$ 表示为两个平方数之和，因为我们已对 $5\cdot 13$ 作了这样的处理.利用上述第1解与公式5，于是得出 $2(5\cdot 13)=9^2+7^2$.类似地，[144] 由第2解可得 11^2+3^2.

乘积的其余部分 $2^6\cdot 3^4\cdot 7^2\cdot 13^2$ 自然是个平方数，故可记为

$$2^6\cdot 3^4\cdot 7^2\cdot 13^2=(2^3\cdot 3^2\cdot 7\cdot 13)^2,$$

将此平方数乘以平方和 9^2+7^2，即得本题的第1解：

$$2^7\cdot 3^4\cdot 5\cdot 7^2\cdot 13^3=(2^3\cdot 3^2\cdot 7\cdot 13\cdot 9)^2 \\ +(2^3\cdot 3^2\cdot 7\cdot 13\cdot 7)^2,$$

或

$$5580731520=(58968)^2+(45864)^2 \\ =3477225024+2103506496.$$

而由 11^2+3^2 导出的本题第2解为：

$$2^7\cdot 3^4\cdot 5\cdot 7^2\cdot 13^3=(2^3\cdot 3^2\cdot 7\cdot 13\cdot 11)^2$$

$$+ (2^3 \cdot 3^2 \cdot 7 \cdot 13 \cdot 3)^2,$$

或

$$5580731520 = (72072)^2 + (19656)^2$$
$$= 5194373184 + 386358336.$$

公式 1 告诉我们本题一共有四解，因为 $4x+1$ 形式的素数 5 与 13，其指数为 $a_1=1, a_2=3$，代入公式后我们将可得出 $(1+1)(3+1)/2=4$. 请读者们自己去找出把 5580731520 表示为两个平方数之和的其他两种办法.†

*　　　*　　　*

如果不限于整数解，则任意整数的平方都可表示为两个平方数之和，且表示法无限多. 当然，解答必须是有理数，即分子、分母都必须是整数. 设我们要求出两个平方数，其和是 3^2，这是一个不含 $4x+1$ 形式素数因子的平方数. 此问题有两解：$\left(\frac{9}{5}\right)^2, \left(\frac{12}{5}\right)^2$ 以及 $\left(\frac{15}{13}\right)^2, \left(\frac{36}{13}\right)^2$，但我们可用如下办法找出许许多多解答，只要我们高兴，想多少就有多少.

由 $X^2+Y^2=Z^2$，可得 $\left(\frac{X^2}{Z^2}\right)+\left(\frac{Y^2}{Z^2}\right)=1$，若 A^2 是给定的平方数，则用它遍乘全式，便得

$$(A^2X^2/Z^2) + (A^2Y^2/Z^2) = A^2.$$

[145]

用第 14 章的毕氏三角形关系式代入，即得出两个合适的分数 $A(m^2-n^2)/(m^2+n^2)$ 与 $2mnA/(m^2+n^2)$，它们各自平方之和为 A^2. 例如，若 $m=2, n=1, m=3, n=2$，即可得出上面的两解.

由于解不受整数的限制，m 与 n 本身也可取分数值，从而可得到形式更简的结果，即

$$A(M^2-1)/(M^2+1), \quad 2MA/(M^2+1),$$

此处，M 可为任意有理分数. 譬如说，若 $A^2=16$，可取 $M=\frac{2}{3}$，

于是有

$$4(-5/9)/(13/9) = -20/13$$

与

$$(2[2/3]4)/(13/9) = 48/13,$$

这两个分数各自平方后，其和即等于 16.

如果我们想求平方后其和为 1 的两个分数，那只要简单地取$(M^2-1)/(M^2+1)$与$2M/(M^2+1)$就行.

*　　　*　　　*

有可能找到三个整数 X,Y,Z，使它们两两平方后相加均是平方数，即：$X^2+Y^2=a^2$，$X^2+Z^2=b^2$，$Y^2+Z^2=c^2$. 例如，$44^2+240^2=244^2$；$44^2+117^2=125^2$；$240^2+117^2=267^2$. 具有长、宽、高为 $44\times117\times240$ 尺寸的长方形盒子，其各面的对角线长度均为整数. 一台数字计算机在最近找出了 130 个这样的三数组.

给出其中某些解的一般公式（不是全部解答）为：

$$X=2mn(3m^2-n^2)(3n^2-m^2),\quad a=2mn(5m^4-6m^2n^2+5n^4),$$
$$Y=8mn(m^4-n^4),\quad b=(m^2+n^2)^3,$$
$$Z=(m^2-n^2)(m^2+n^2+4mn)\times(m^2+n^2-4mn);\quad c=(m^2-n^2)(m^4+18m^2n^2+n^4).$$

上面的三数组相当于 $m=2,n=1$ 的情况.

*　　　*　　　*

关于平方数的一个令人惊讶的事实是：任一正整数均可表示为至多四个平方数之和. 证明这个定理并不简单. 许多正整数可用个数较少的平方数之和来表达. 当然，所有的平方数都是一个平方数之"和"，我们已经知道，2^nQ^2P（此处 P 为 $4x+1$ 形式的素数之积）形状的数可表示为两个平方数之和. 所有其他正整数除去以下例外均可表示为三个平方数之和，只有 $4^a(8x+7)$ 形状的特殊正整数，例如 7，28，60，92 等才需要用四个平方数之

[146]

和来表达.

* * *

数论的一个美妙分支探讨“二次剩余”，即平方剩余问题，我们将在第 19 章中加以讨论.

* * *

有一类正整数称为“自守数”，这类数目平方之后，最后 x 位数码与原数的最后 x 位一样. 例如，在 $x=1$ 时，任意一个以 5 结尾的正整数平方之后末位数也是 5；$x=2$ 时，末两位为 25 的正整数，其平方数的末两位必然也是 25；$x=3$ 时，以 625 为最后三位的任意正整数的平方，最后三位也肯定是这三个数码. 对 $x=1,2,3$ 来说，另一种解答是 6，76，376. 这些数的平方同样也具有类似的尾数. 自守数的尾数现已计算到很多位数，例如，对十进位数而言，唯一的两个 16 位自守数是 6259918212890625 与 3740081787109376. 除此以外，还有很肤浅平凡的例子，以若干个 0 结尾或在许多个 0 后面接着 1 的数，其平方数当然也有同样的尾巴.

非十进制数中也有自守数，例如对 6 进位数而言，七位自守数有两个，非此即彼，它们是 1350213 与 4205344. 在基数为 p 的进位制中，n 位自守数必需遵从规律：

$$x^2 \equiv x \mod p^n.$$

* * *

平方数与构成它的数码之间有着许多值得注意的关系. 譬如说，在平方数 2025 的每个数码上都加 1，得出的四位数 3136 依旧是平方数. 显然，二位平方数 25 也有类似性质.

把 65 的数码逆序书写，得出 56，此时便有 $65^2-56^2=33^2$；对二位数来说，具有此种关系的仅此一家而已.

表 64 列出了具有九位数码，不重不漏的特殊平方数；表 65 则列出了十位数码的特殊平方数. 实际上这只是其中的一部分

[147] 例子.表 64 共有 83 例,而表 65 则有 87 例.

$11826^2=139854276$	$19629^2=385297641$	$25059^2=627953481$
$12363^2=152843769$	$20316^2=412739856$	$25572^2=653927184$
$12543^2=157326849$	$22887^2=523814769$	$25941^2=672935481$
$14676^2=215384976$	$23019^2=529874361$	$26409^2=697435281$
$15681^2=245893761$	$23178^2=537219684$	$26733^2=714653289$
$15963^2=254817369$	$23439^2=549386721$	$27129^2=735982641$
$18072^2=326597184$	$24237^2=587432169$	$27273^2=743816529$
$19023^2=361874529$	$24276^2=589324176$	$29034^2=842973156$
$19377^2=375468129$	$24441^2=597362481$	$29106^2=847159236$
$19569^2=382945761$	$24807^2=615387249$	$30384^2=923187456$

表 64 含有九位不重复数码的平方数

$32043^2=1026753849$	$45624^2=2081549376$
$32286^2=1042385796$	$55446^2=3074258916$
$33144^2=1098524736$	$68763^2=4728350169$
$35172^2=1237069584$	$83919^2=7042398561$
$39147^2=1532487609$	$99066^2=9814072356$

表 65 含有十位不重复数码的平方数

在一本古老破旧的《圣经》活页上记录了一些关系式,它表明两个平方数的差是一个九数码齐全,不重不漏的数,我们将它摘录如下:

$$11113^2-200^2=11313\cdot 10913=123458769$$
$$31111^2-200^2=31311\cdot 30911=967854321$$
$$11117^2-200^2=11317\cdot 10917=123547689$$
$$11356^2-2000^2=13356\cdot 9356=124958736$$
$$12695^2-6017^2=18712\cdot 6678=124958736$$
$$16260^2-11808^2=28068\cdot 4452=124958736$$
$$12372^2-300^2=12672\cdot 12072=152976384$$

表 66 含有九个数码的平方差

请注意前二例中,第一个平方数,第一个因子以及最后的结果都是互为逆序数的.

计算机何以要利用这些数码的特殊组合,情况尚不甚清楚.

[148] 但是,大于 1 的任何奇数,作为 4 的倍数(4 本身要除外)的任何

偶数都可表示为两个平方数之差.或许用单调递增或单调递减的数码来作为例子更有趣些,以下便是本书作者得到的结果:

$$
\begin{aligned}
123456789 &= 3^2 \cdot 3607 \cdot 3803 = 61728395^2 - 61728394^2 \\
&= 20576133^2 - 20576130^2 \\
&= 6858715^2 - 6858706^2 \\
&= 18917^2 - 15310^2 \\
&= 18133^2 - 14330^2 \\
&= 11115^2 - 294^2, \\
987654321 &= 3^2 \cdot 17^2 \cdot 379721 = 493827161^2 - 493827160^2 \\
&= 164609055^2 - 164609052^2 \\
&= 54869689^2 - 54869680^2 \\
&= 29048665^2 - 29048648^2 \\
&= 9682911^2 - 9682860^2 \\
&= 3227705^2 - 3227552^2 \\
&= 1708889^2 - 1708600^2 = 570015^2 - 569148^2 \\
&= 191161^2 - 188560^2.
\end{aligned}
$$

有趣的是,值得指出 9 个数码的全排列总数为 $9! = 362880$. 其中的四分之一,即 90720 个正整数具有 $4x+2$ 的形状,即结尾为 02,06,10,14,…,98 的整数,它们是无法表示为两数平方差的.加上 1 与 4 之后,共有 90722 个数不能作此种表示.剩下来的还有 272158 个九数码齐全,不重不漏的数可以表示为两数的平方差.因此,破旧《圣经》上的表格,远远谈不上完整,不值得破格重视.

* * *

平方数以及平方数表在数的因式分解中有很大用处.例如,既然形式为 $4x+1$ 的任一素数都可表示为两个平方数之和,这样两个素数的乘积就可用两种方法表示为两个平方数之和,这已在公式 3 中提到过.于是有:

1. 若一奇数可用两种方式表示为两平方数之和,则它必为

合数，并且有办法找出它的因子（见第 21 章）．如果两个平方数不互质，那就立即可以知道其公因子即是该数的一个除数．

2．如一奇数可唯一地表示为两个互质的平方数之和，则它必是一个素数或其乘幂．若该数能表示为两个具有公因子的平方数之和，则该数不可能是素数或素数的平方，但肯定是素数的某个高次方幂．公因子本身也是素数的一个乘幂．

3．如一性质不明之数为 $4x+1$ 形式，且不能表示为两个平方数之和（连一种方法都找不到），则它必为合数，具有偶数个素因子，每个都取 $4x-1$ 形状．

4．如一性质不明之数为 $4x-1$ 形式，且在任何情况下都不能表示为两个平方数之和，则用以判定一数是否为素数的平方和测试法对它无效．

让我们来看一下数 221．用此数减去平方数，从 196 开始，我们立即得出余数 25，即 $221=196+25=14^2+5^2$．继续做下去，又可得到 $221-121=100$，即 $221=11^2+10^2$．这就肯定表明 221 是个合数，因为它可用两种方法表示为两数的平方和．至于求出其实际因子的办法，我们将推迟到第 21 章再讲．

再看数 229，减去平方数后，我们马上找到关系式 $229=15^2+2^2$，继续做下去，我们只需进行到 11^2，这时留下的余数略小于原数的一半．测试结果肯定了不存在和为 229 的其他两个平方数，因而表明 229 肯定是个素数．

数 77 尽管具有 $4x+1$ 的形状，但用上述测试方法，它无法表示为两个平方数之和．因而 77 是合数，其因子为 7 与 11，每个因子都具有 $4x-1$ 形状．

再去检查 223，它具有 $4x-1$ 形式；因此不必徒劳无益地想把它表示为平方和，要依靠其他办法去分解因子．

当然，此种办法不会应用到上面所说的那些很小的自然数上去．设想我们要分解数 16000001 的因子，如第 14 章表 58 所示（$T=8000000$，$2T+1$ 必需分解因子），计算构成 8000000 个

毕氏三角形的一边的可能个数时，此种分解是必须进行的、可供利用的，由雷默所编制的因数表只有上到一千万为止；因此分解因子只好利用上述平方和办法. 正好碰巧，16000001 一眼即可看出来是$(4000)^2+1^2$；因而如能找到这一和数的另外两个平方数，即可判明该数为合数并分解出其因子. 末二位的平方数尾数表格显示，此种平方数的结尾必须是 00，01，25，76，这样才能在 16000001 减去它们之后留下合适的尾数. 为了方便起见，当然可以利用末三位的平方数尾数(它们当然远远不止 22 个). 这样一来，测试次数自然可以大为减少. 若再应用一张较大的平方数表，我们即可在数分钟内发现 $16000001-1049^2$ 是一个平方数，即 [150]

$$16000001 = 4000^2 + 1^2 = 1049^2 + 3860^2.$$

游戏做好了，此数已被我们擒获，几分钟之内，我们已判明它是 229 与 69869 的乘积. 在因子数表中检查一下后面两数(自然也可继续利用上面的办法)，可以发现 229 是素数，而 69869 可继续分解为 641 与 109 的乘积，因而 $16000001=229\cdot641\cdot109$.

*　　　*　　　*

在第 14 章中我们已给出了两个平方数之和仍是平方数的公式. 另外还有三个或更多个整数平方加起来仍能得出整数平方的式子. 例如，$x^2+y^2+z^2=w^2$ 的一个解为

$$\begin{aligned} x &= p^2 + q^2 - r^2, \\ y &= 2pr, \\ z &= 2qr, \\ w &= p^2 + q^2 + r^2. \end{aligned}$$

这里的 p，q，r 不一定要求是有理数. 表 67 给出了利用这些公式的某些结果：

p	q	r	x	y	z	w	三个平方数之和是一平方数
1	1	1	1	2	2	3	$1^2+2^2+2^2=3^2$
$\sqrt{2}/2$	$3\sqrt{2}/2$	$\sqrt{2}$	3	2	6	7	$3^2+2^2+6^2=7^2$
1	2	2	1	4	8	9	$1^2+4^2+8^2=9^2$
2	3	4	−3	16	24	29	$3^2+16^2+24^2=29^2$

表 67　等于三个平方数之和的平方数

[151]　　　　* 　　　* 　　　*

平方数有个神奇关系：从 $n(2n+1)$ 的平方开始的 $(n+1)$ 个连续数的平方数，其和正好等于其后 n 个连续数的平方数之和.

n	
1	$3^2+4^2=5^2$
2	$10^2+11^2+12^2=13^2+14^2$
3	$21^2+22^2+23^2+24^2=25^2+26^2+27^2$
4	$36^2+37^2+38^2+39^2+40^2=41^2+42^2+43^2+44^2$
5	$55^2+56^2+57^2+58^2+59^2+60^2=61^2+62^2+63^2+64^2+65^2$

表 68　宝塔式的连续平方和

许多连续平方数之和仍是一个平方数，这有不少办法可以获得此种结果. 表 69 给出了一些实例.

$$1^2+2^2+3^2+\cdots+24^2=4900=70^2$$
$$18^2+19^2+20^2+\cdots+28^2=5929=77^2$$
$$25^2+26^2+27^2+\cdots+50^2=38025=195^2$$
$$38^2+39^2+40^2+\cdots+48^2=20449=143^2$$
$$456^2+457^2+458^2+\cdots+466^2=2337841=1529^2$$
$$854^2+855^2+856^2+\cdots+864^2=8116801=2849^2$$

表 69　若干个连续平方数之和仍是一个平方数

除去连续数外，也可以有其他算术级数的若干项，其平方和仍是一平方数，例如

$$2^2+5^2+8^2+11^2+14^2+17^2+20^2+23^2+26^2=48^2.$$

在离开本话题前，我们尚应提一提立方数之间的奇妙联系：

若干个连续立方数之和还是一个立方数，例如：

$$3^3+4^3+5^3=6^3,$$
$$6^3+7^3+8^3+\cdots+69^3=180^3,$$
$$1134^3+1135^3+1136^3+\cdots+2133^3=16830^3.$$

*　　*　　*

三个平方数可以形成算术级数，但四个或更多个平方数就不行.后一部分的证明是困难的.为了找出能形成算术级数的三个平方数 X^2,Y^2,Z^2，我们可从 $Y^2-X^2=Z^2-Y^2$ 着手，即 $2Y^2=X^2+Z^2$. 令 $X=p-q, Z=p+q$，则 $X^2+Z^2=2(p^2+q^2)$，于是 $Y^2=p^2+q^2$，这就是第14章中给出的毕氏三角形基本关系式. 故得 $p=m^2-n^2$；$q=2mn$；$Y=m^2+n^2$；$X=m^2-n^2-2mn$；$Z=m^2-n^2+2mn$.（若另外设 $p=2mn$；$q=m^2-n^2$；此时 Y,Z 不变，而 X 变为 $2mn-(m^2-n^2)$；以上两结果可合并记为 $X=\pm[m^2-n^2-2mn]$.）表70给出了一些形成算术级数的平方三数组. [152]

m	n	X	Y	Z	X^2	Y^2	Z^2	公差
2	1	∓ 1	5	7	1	25	49	24
3	2	∓ 7	13	17	49	169	289	120
4	1	± 7	17	23	49	289	529	240
4	3	∓ 17	25	31	289	625	961	336
5	2	± 1	29	41	1	841	1681	840

表70　形成算术级数的三个平方数

数学家弗兰尼格(Frenicle)用一种简洁的说法描述了组成算术级数的三个平方数：中间的一数 Y 是毕氏三角形的斜边，最小的一数 X 是差数，最大的一个 Z 是这种三角形的两直角边之和，也就是上文所提到的 $Y=m^2+n^2$；$X=m^2-n^2-2mn$；$Z=m^2-n^2+2mn$.

在某些问题中先给出公差 d，而要求三个能形成算术级数的平方数，但不一定非要整数解不可.此时将有关系式：Y^2-

$X^2=d=(m^4+2m^2n^2+n^4)-(m^4+n^4+4m^2n^2-4m^3n-2m^2n^2+4mn^3)=4mn(m^2-n^2)$. 整数或分数解可能不存在，即便存在，也不易求得. 由表 70 可知，当平方数为整数时，公差必可被 24 整除. 对整数解来说，这是一个必要条件.

例如，设 $d=240$，要在 $240=4mn(m^2-n^2)$，亦即 $60=mn(m^2-n^2)$ 中解出 m,n，由试探法可找到 $m=4,n=1$ 是满足该方程的一个解.

若 d 不是 24 的倍数，则不可能有整数解，但有时可得分数解. 例如，设 $d=5$，

[153]

$$5=4mn(m^2-n^2).$$

或者说，

$$5K^2=4MN(M^2-N^2)$$

能否有解呢？上式可改写为

$$5=4(M/\sqrt{K})(N/\sqrt{K})[(M/\sqrt{K})^2-(N/\sqrt{K})^2].$$

于是，$m=M/\sqrt{K}$，$n=N/\sqrt{K}$，由此可得出 X,Y,Z 的分数解. 无理数 $\sqrt{K}$ 在 X,Y,Z 中将会消失，因为在它们的表达式中出现的都是二次幂. 方程 $5K^2=4MN(M^2-N^2)$ 通过试探法求得的一个解是 $5\cdot 12^2=4\cdot 5\cdot 4(5^2-4^2)$. 从而 $m=5/\sqrt{12}$，$n=4/\sqrt{12}$，代入 X,Y,Z 的公式，从而可得出 $X=-31/12$，$Y=41/12$，$Z=49/12$，于是

$$(1681/144)-(961/144)=(2401/144)-(1681/144)$$
$$=(720/144)=5,$$

这就表明，$\frac{961}{144}$，$\frac{1681}{144}$，$\frac{2401}{144}$ 能形成一个算术级数，其公差是 5.

*　　　　*　　　　*

1739—1740 年的《女士日记》中有一道趣题，现在的读者们

解起来不会有什么困难.此题谈到三个荷兰人同他们的老婆到市场里买猪的故事.

男人的名字叫亨利,埃利,康纳里斯;女人的名字叫盖特路德,凯塞林,安娜.每个人买进的猪的头数同他或她为每头猪付出的价钱一样多,而每个男人比他的老婆多支出 63 元.已知亨利比凯塞林多买 23 头猪,埃利比盖特路德多买 11 头猪.试问:谁同谁是夫妻? †

有个类似的问题讲到五位母亲同她们的女儿.这十个妇女,每人都买了若干码布,码数正好等于她为每码布所支付的价钿(单位为"分"),每位母亲都比她女儿多用掉 4.05 元.鲁滨逊夫人比伊文思夫人多用去 2.88 元,而后者所用的钱只是琼斯夫人的四分之一.史密斯夫人用得最多.布朗夫人比贝茜姑娘多买 63 码布,安娜比玛丽多买 48 码,她比埃米莉多用掉 29.12 元.还有一个姑娘的教名叫艾达.请问,她姓什么? †

据说此题曾一度投给澳大利亚悉尼市的一家晚报,因为它开设了一个"提高智力"的专栏,但不久就遭到退稿,其理由是太孩子气,而且报纸只能刊登有解答的题目. [154]

* * *

有一个古老问题涉及所谓"相合数",它曾被中世纪阿拉伯人探讨过,同本书第 25 章的 59 题"约翰·史密斯船长与其后裔"的趣题也有联系.数 k 称为"相合"的,如果存在着整数 x 与 y,能使 x^2+ky^2 与 x^2-ky^2 均为平方数.表达式 x^2-ky^2 可允许是一个负平方数,因为由此负解常可推出一个相伴的正解.尽管现在已有不少威力巨大的解析工具可供我们自由调遣,仍然没有确切办法来求出一个给定数的相合数.即使我们已经知道 k 是相合数,求起解来也很困难.对小于 100 而且不含平方因子的 k 值,可能的相合数只有 36 个,它们是:5,6,7,13,14,15,21,22,23,29,30,31,34,37,38,39,41,46,47,53,55,61,62,65,69,70,71,77,78,79,85,86,87,93,94,95.为什么要不考虑平方因

子呢？这是由于若 k 不含平方因子而 $x^2+ky^2=u^2$，$x^2-ky^2=v^2$ 均有解，则对一个新的常数 $K=kL^2$ 而言，所得之结果仍必有解. 因此时可改写 $L^2x^2+kL^2y^2=L^2u^2$，$L^2x^2-kL^2y^2=L^2v^2$，即 $(Lx)^2+Ky^2=(Lu)^2$，$(Lx)^2-Ky^2=(Lv)^2$. 因此，若 k 是相合数的话，则 kL^2 也必是相合数. 于是，在 100 以下的自然数中，可以再追加 14 个含平方因子的相合数，它们是：20，24，28，45，52，54，56，60，63，80，84，88，92，96. 剩下的 49 个正整数，其中包含 1 与 2，是不相合的. 故知 $x^2+y^2=u^2$ 与 $x^2-y^2=v^2$ 无解，$x^2+2y^2=u^2$ 与 $x^2-2y^2=v^2$ 亦然.

已经证明形如 $8x+3$ 的素数或两个此类数目的乘积是不相合的；对素数 $8x+5$ 的二倍或者两个这种数目乘积的二倍也是不相合的. 如果不存在一个数 m，它小于已知素数 k 的一半，而能使 m^2+1 或 m^2-2 被 k 整除，则素数 k 是不相合的.

对最小的相合数 5 来说，有一个解是 $41^2+5\cdot12^2=49^2$，$41^2-5\cdot12^2=31^2$. 如果第二个方程准许有负数解，则本题尚可以写出一个更小一些的解：$2^2+5\cdot1^2=3^2$，$2^2-5\cdot1^2=-1^2$. 下[155]文将要说到，从这种负数解总可以得出相伴的正数解. 满足 $x^2+5y^2=u^2$，$x^2-5y^2=v^2$ 的下一组数值是 $x=3344161$；$y=1494696$；$u=4728001$，$v=1494696$. 第三个"最小解"就一点也不小了，它们是：

$$x = 654686219104361;$$
$$y = 178761481355556;$$
$$u = 767067390499249;$$
$$v = 518493692732129.$$

前已讲过，给定公差 d，求三个平方数，使之形成算术级数，此时将引出方程 $dK^2=4MN(M^2-N^2)$. 设 d 是素数，则 M,N,K 可视为互质，因若有公因子的话，一定可以消去. 由于 M^2-

N^2，M，N 是互质的，这三个因子中的两个必须是平方数，而第三个是平方数的 d 倍，这样才能符合方程的左边式子. 设 N 是一个平方数，记为 p^2；M^2-N^2 也是一个平方数，记作 q^2；于是 $M=dr^2$，把 M 与 N 代入表达式 $M^2-N^2=q^2$，结果就得出 $d^2r^4-p^4=q^2$. 于是

$$(dr^2+p^2)(dr^2-p^2)=q^2.$$

由于 p,q,r 互质，这些因子的最大公因数不能超过 2，所以上式左边的每个因子或者是一个平方数，或者是平方数的二倍. 在前一种情况下即得 $dr^2+p^2=u^2$；$dr^2-p^2=v^2$，它们可改写为：

$$p^2+dr^2=u^2,$$
$$p^2-dr^2=-v^2.$$

由此即可得出结论：d 必须是相合数. 已知在 $d=5$ 时，$p=2$；$r=1$；$u=3$；$v=1$. 从而有

$$N=p^2=2^2;\ M=5r^2=5\cdot 1^2;$$
$$M^2-N^2=q^2=u^2v^2=3^2\cdot 1^2.$$

于是 $5K^2=4\cdot 5\cdot 4\cdot 3^2$，故 $K=12$，同以前一样得到 $M/\sqrt{K}=5/\sqrt{12}$，$N/\sqrt{K}=4/\sqrt{12}$，代入后即得出公差为 5，且能形成算术级数的三个平方数：

$$(31/12)^2,(41/12)^2,(49/12)^2.$$

上面已经说过，当 $x^2-ky^2=-v^2$ 成立时，另一个正平方数 [156] 解 v^2 也可求出. 这可由下面支配一切相合数的一般法则推导而得. 在求解

$$X^2+abY^2=Z^2,$$
$$X^2-abY^2=W^2$$

时，可先求出辅助方程

$$ax^2 + by^2 = nz^2,$$
$$ax^2 - by^2 = \pm nw^2$$

的解，然后即得 $X = n(z^4 + w^4)/2$，$Y = 2xyzw$.

例如，设 $a = 1$，$b = 5$，$n = 1$，而 $x^2 + 5y^2 = z^2$ 以及 $x^2 - 5y^2 = \pm w^2$. 由试探法可得出解 $2^2 + 5 \cdot 1^2 = 3^2$，$2^2 - 5 \cdot 1^2 = -1^2$，于是 $x = 2$，$y = 1$，$z = 3$，$w = 1$. 从而 $X = (3^4 + 1^4)/2 = 41$；$Y = 2 \cdot 2 \cdot 1 \cdot 3 \cdot 1 = 12$，故有 $41^2 + 5 \cdot 12^2 = 49^2$，$41^2 - 5 \cdot 12^2 = 31^2$，现在第二方程右边的平方数就是正的了. 我们也可继续做下去而得 $X_1 = (49^4 + 31^4)/2 = 3344161$，$Y_1 = 2 \cdot 41 \cdot 49 \cdot 31 = 1494696$，以此类推……

相合数 47，53，61 的每一个都需要有 16 位数作为对偶方程中 x 的最小解. 而相合数 79 更进一步，需要一个 17 位数作最小解. 在方程 $x^2 + 101y^2 = u^2$ 与 $x^2 - 101y^2 = v^2$ 中，满足方程的最小解为：

$$x = 2015242462949760001961,$$
$$y = 118171431852779451900,$$
$$u = 2628124370727269996961,$$
$$v = 2339148435306225006961.$$

涉及相合数有趣性质的进一步讨论不打算进行下去了. 如果读者能找到三个能形成算术级数，而公差为 23 的有理数平方（整数解在此情况下不可能），他无疑已经熟练掌握了本话题所提及的知识内容. †

* * *

尽管近年来已做了许多工作，问题依然没有彻底解决，这就是把矩形分割为若干个不同的正方形问题. 各正方形面积之和等于矩形的面积，这个条件是不充分的. 因为任何正整数均可表 [157]

示为至多四个整数平方之和.需要把各个正方形几何地组装为矩形,其特例是组装成正方形.例如数78,相当于边长为6与13的矩形,它是等于 $7^2+5^2+2^2$ 的,但这些正方形放不到一起,如不通过切割,是形成不了给定尺寸的矩形的.数78也可拆成 $8^2+3^2+2^2+1^2$ 或 $6^2+5^2+4^2+1^2$,但它们也都拼不成 6×13,3×26 或 2×39 的矩形.只有某些矩形(其面积是合数)才能分割成不同的正方形.试问:此类合数有什么独特性质?

若此种分解可能,则它将不少于九个不同正方形才能做到.现已证明,矩形不能分割为比九个更少的正方形.直至最近,一直未能发现正方形能分割成不同的正方形,好不容易才有了 [158] 1015^2 这个例子,它可以分解为下列28个正方形:

$$\begin{aligned}&2^2+18^2+22^2+37^2+38^2+39^2+41^2+43^2+49^2+67^2\\&\quad+72^2+80^2+85^2+103^2+116^2+154^2+164^2+175^2\\&\quad+178^2+192^2+200^2+207^2+215^2+222^2+230^2\\&\quad+247^2+422^2+593^2.\end{aligned}$$

把这些东西组装成边长为1015的正方形着实要有点本事!图8A给出了具体的组装法.

对这个1015的平方还有一解,同样有28块,下面便是此等正方形的边长:13;16;17;23;30;43;47;84;92;93;119;120;142;163;165;167;177;183;188;199;215;219;261;270;280;363;372;382.

边长为608的正方形可以分割为较小的、不同的26块正方形.此问题的解以及边长为1015的正方形分割成28块以后的组装问题,请读者们不妨尝试一下.

边长175,面积为30625的正方形可以分割为24块不同的正方形.迄今为止,它是本书作者所知的正方形被分解为不同正方形的最少块数.从左上角按反时针方向转,构成边界的九个正方形是 $55^2,56^2,64^2,33^2,35^2,43^2,51^2,81^2,39^2$.有些线索作为暗

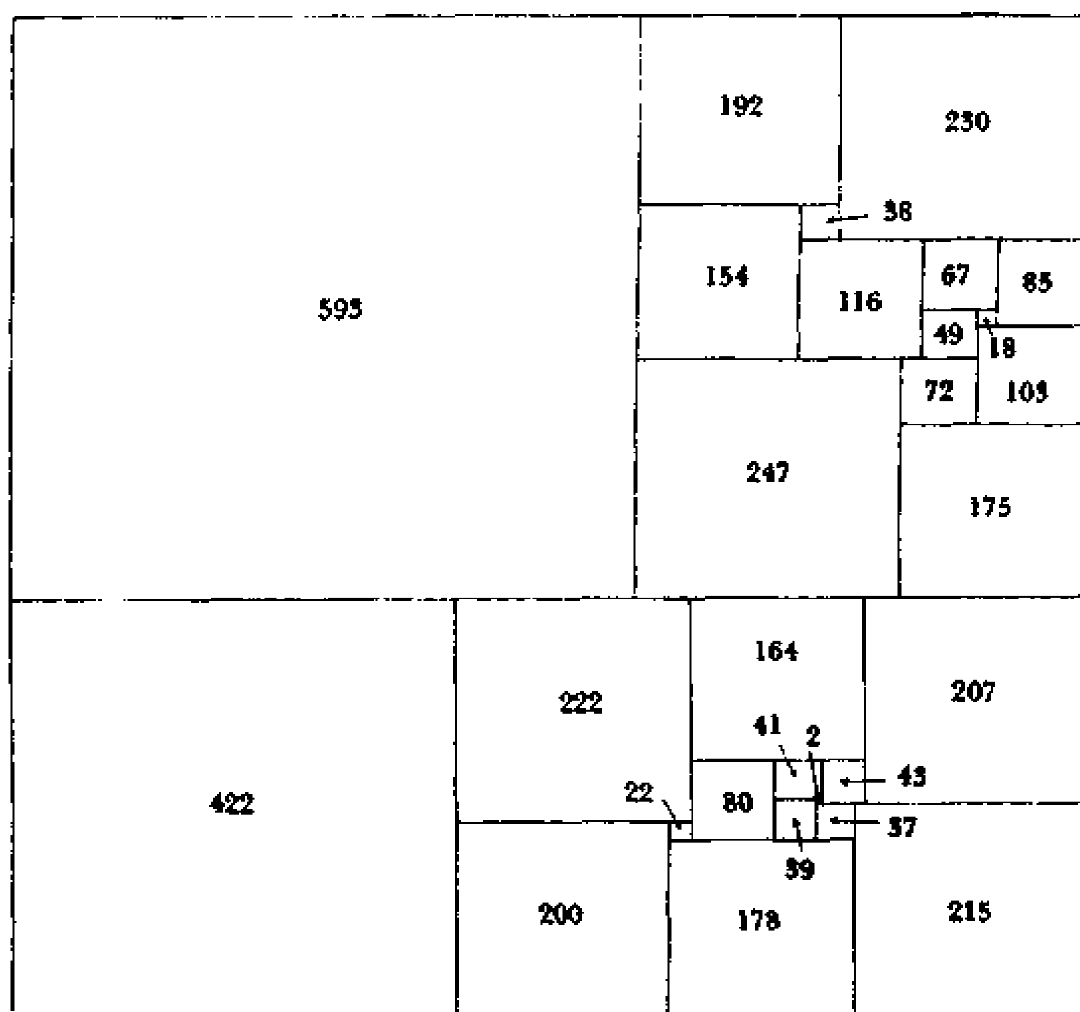
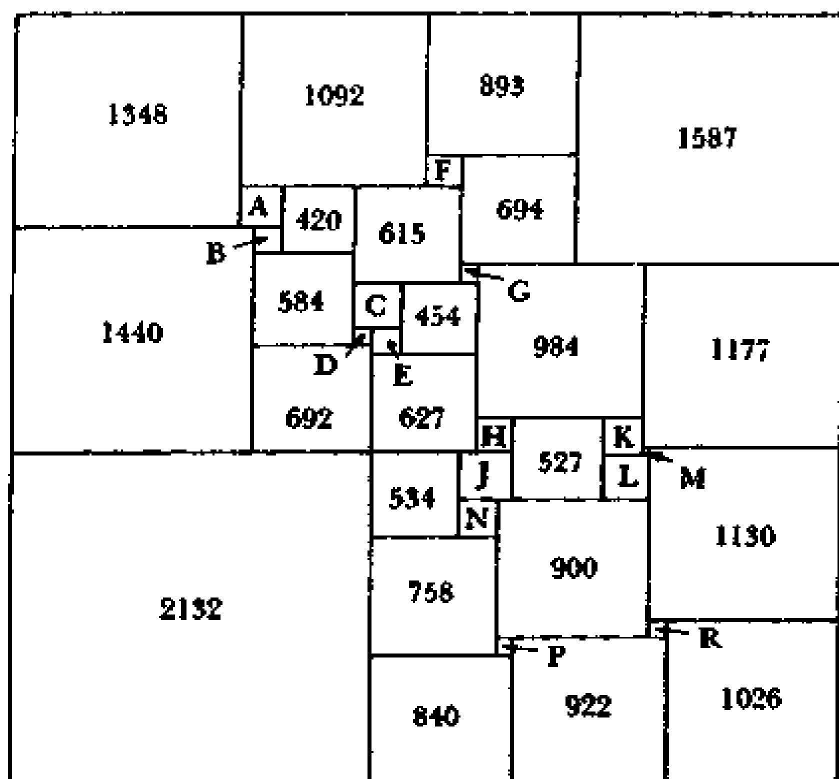


图 8A 由 28 个不同正方形组装成的大正方形

示，读者们把剩下的 15 块正方形：$1^2,2^2,3^2,4^2,5^2,8^2,9^2,14^2$，$16^2,18^2,20^2,29^2,30^2,31^2,38^2$进行装配，大概不会有多大困难了.

有一个很奇怪的正方形，边长为 4920，面积为 24206400，它可分解为 38 个不同正方形. 形成边界的 11 个正方形是：1348^2，$1440^2,2132^2,840^2,922^2,1026^2,1130^2,1177^2,1587^2,893^2,1092^2$，也是从左上角按反时针方向轮转. 剩下来的正方形，其边长为 47，82，104，108，120，164，173，199，217，224，240，256，281，287，310，420，454，527，534，584，615，627，692，694，758，900，984. 请参看附图 8B.



$A=256$	$D=108$	$G=120$	$K=240$	$N=224$
$B=164$	$E=173$	$H=217$	$L=287$	$P=104$
$C=281$	$F=199$	$J=310$	$M=47$	$R=82$

图 8B 由 38 个不同正方形组装成的大正方形

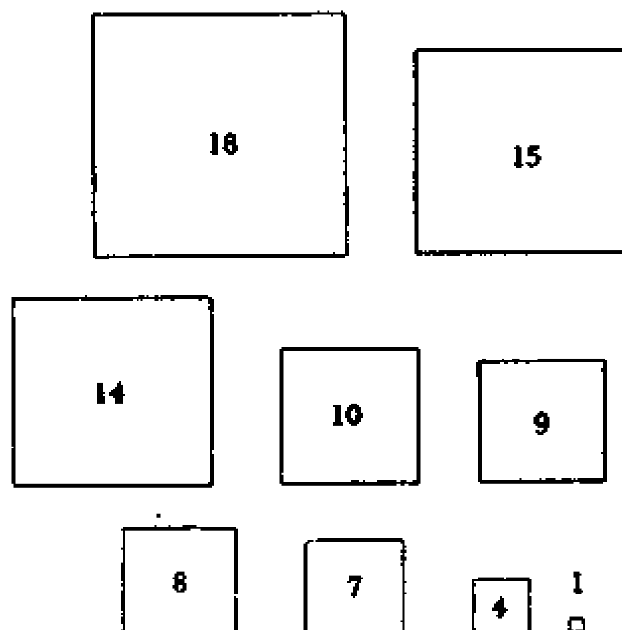


图 8C 要求用图中的 9 个正方形组装成一个矩形 [160]

以数 1056 为面积的矩形可分解为九个不同正方形，其边长如图 8C 所示. 读者们能重新把它们组装成矩形吗？†

稍有不同的问题是把正方形分解为个数最少的正方形，但允许其中有相同的. 当然，仅仅在数值上相等是不够的，小正方形必须在几何上拼装成大正方形. 边长为 13 的正方形可分解为 [159] 若干个，其中有大小一样的正方形，例如，一块正方形的边长为 12，另外 25 块都是单位正方形. 另一种分解法是 $1\cdot 10^2+7\cdot 3^2+6\cdot 1^2$. 前一种办法需要分割成 26 个正方形，而后一种则为 $1+7+6=14$ 个正方形. 试问：怎样才能使分割成的正方形块数最少？†

* * *

阶乘公式引出一个涉及正方形的难题. 如果我们审视第 7 章表 22 中以 $(n-1)!+1$ 开头的那一列，就能看到 25 与 121 是平方数，即 $4!+1=25=5^2$，而 $5!+1=121=11^2$. 除此之外，还有 $7!+1=5041=71^2$. 除去 $x=4,5,7$ 之外，一般地说，$x!+1=Y^2$ 还有没有解呢？对此问题，人们一直追查到 $x=1020$ 为止都没有发现新解. 如果真有此种解存在，它们肯定庞大无比；即便是 100！，它也有 158 位，而 1020！的位数超过 2600.

* * *

一讲到平方数，人们就会指出：前 n 个连续正整数之和的平方等于这些数各自立方之和，即 $(1+2+3+\cdots+n)^2=1^3+2^3+3^3+\cdots+n^3$，由于 $1+2+3+\cdots+n$ 是一算术级数，其和为 $\frac{n(n+1)}{2}$，因而有 $1^3+2^3+3^3+\cdots+n^3=[n(n+1)/2]^2$. 另一方面，连续正整数的平方和有下列关系式

$$1^2+2^2+3^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}.$$

* * *

已故犹太学校[1]的教师耶库梯尔·琴斯保博士(Dr. Jekuthiel Ginsburg)注意到6的除数为1,2,3,6,而它们又各有1,2,2,4个除数.这些数之间具有关系式$(1+2+2+4)^2=1^3+2^3+2^3+4^3$.另外30的除数为1,2,3,5,6,10,15,30,而它们的除数个数为1,2,2,2,4,4,4,8.且有下述关系成立:

$$(1+2+2+2+4+4+4+8)^2 \\ =1^3+2^3+2^3+2^3+4^3+4^3+4^3+8^3=729.$$[2]

*　　*　　*

另一种,类型略有不同的关系是:

$$2(1+2+\cdots+n)^4=(1^5+2^5+\cdots+n^5) \\ +(1^7+2^7+\cdots+n^7).$$

*　　*　　*　　[161]

三角形数是指具有$a(a+1)/2$形式的数.我们采用记号$\sum_1^n a(a+1)/2$表示n个三角形数之和,a的取值自1到n,于是有:

$$3\left[\sum_1^n a(a+1)/2\right]^3=\sum_1^n[a(a+1)/2]^3+2\sum_1^n[a(a+1)/2]^4.$$

例如,$n=3$时有关系式

$$3(1+3+6)^3=1^3+3^3+6^3+2(1^4+3^4+6^4)=3000;$$

而$n=4$时有关系式

$$3(1+3+6+10)^3=1^3+3^3+6^3+10^3+2(1^4+3^4+6^4+10^4)$$

---

① 指犹太教神学研究与世俗学科相结合的学校.解放前,上海陕西北路(原名西摩路)也曾经有过此种学校;后被日本人侵占,沦为日本侵略军的集中营.——译者注.

② 这个奇异性质远远不限于6与30,对其他一大批自然数也都适合,例如香港回归的特征数199771.——译者注.

$$=24000,$$

等等,依此类推.

* * *

这里还有一些平方数"奇观":

$$12345678987654321 = (111111111)^2,$$
$$278886^2 = 77777400996,$$
$$278887^2 = 77777958469.$$

* * *

不难找到一些平方数,其和等于另外一些平方数之和,例如 $4^2+5^2+6^2=8^2+3^2+2^2$. 格外值得注意的是这些关系竟然对好几个乘幂都能成立,例如

$$1^n+4^n+5^n+5^n+6^n+9^n=2^n+3^n+3^n+7^n+7^n+8^n$$

对 $n=1,2,3$ 均是正确的.这种关系称为"多次或多度等幂".记号 $\stackrel{n}{=}$ 用来表示使和式成立的幂指数的限度;例如,上述"三度"成立的关系式,可以简单地记为:$1,4,5,5,6,9 \stackrel{3}{=} 2,3,3,7,7,8$. 这就节省了各个幂指数的书写.更为令人惊讶的是五度等幂和关系 $0,5,6,16,17,22 \stackrel{5}{=} 1,2,10,12,20,21$;$1,11,13,33,35,45 \stackrel{5}{=} 3,5,21,25,41,45$. 如果把两个式子的对应项相加,则还能得出 $1,16,19,49,52,67 \stackrel{5}{=} 4,7,31,37,61,64$. 另外的五度等幂和关系有 $1,5,10,18,23,27 \stackrel{5}{=} 2,3,13,15,25,26$;以及 $1,6,7,17,18,23 \stackrel{5}{=} 2,3,11,13,21,22$. 为了更一般起见,让我们用文字代替数字,于是就有 $a,(a+4b+c),(a+b+2c),(a+9b+4c),(a+6b+5c),(a+10b+6c) \stackrel{5}{=} (a+b),(a+c),(a+6b+2c),(a+4b+4c),(a+10b+5c),(a+9b+6c)$. [162] 最后,我们还有更惊人的七度等幂和关系:$1,13,28,70,82,124,139,151 \stackrel{7}{=} 4,7,34,61,$

91,118,145,148.

有时候,等幂和关系仅仅对偶次幂成立,例如 1,2,31,32,55,61,68 $\stackrel{2n}{=}$ 17,20,23,44,49,64,67(n=1,2,3,4,5).[①]

在选择等幂和关系式中各项时有很大的选择余地,例如 43,61,67 $\stackrel{2}{=}$ 47,53,71;127,149,151 $\stackrel{2}{=}$ 131,139,157;281,281,1181,1181 $\stackrel{3}{=}$ 101,641,821,1361. 有关各项都是素数.

我们也有办法使各平方数之和仍是一平方数,例如在关系式 1,14,24,27,52,57,63,74 $\stackrel{2}{=}$ 5,10,20,31,48,61,67,70 中,各项平方数之和是 130^2,但是,一次方的和当然不是平方数. 另一个例子是 27,30,40,53,76,87,93,98 $\stackrel{2}{=}$ 28,33,39,50,73,86,96,99,这里,平方数的和是 194^2.

* * *

等幂和中的数码,有时竟可作为生成子,以使得经过适当组合以后,正序书写与逆序书写的各数仍具有等幂和关系. 例如,我们可从

$$4^2+5^2+6^2=8^2+3^2+2^2$$

开始,在等式两边先左后右地取各个数码的任意组合,从而得到 48,53,62. 把这些二位数逆序书写,于是得到 84,35,26. 此时即有关系式 $48^2+53^2+62^2=84^2+35^2+26^2$ 成立. 继续按此进行,我们也可改用 48,52,63;43,58,62;43,52,68;42,58,63;42,53,68. 每一组三数组,其平方和等于各逆序数的平方之和. 这里共有 $3\times2\times1=3!$ 种排列,于是可以写出六个等式.

此种关系也可以推广到项数更多的场合. 例如,若以 8,5,

① 原文如此. 经译者演算,此关系式不能成立. 本书再版时亦未改正. 而本章后附之有关参考文献、载有此等论文之杂志,国内各大学图书馆中大都未收藏. 特此指出,以待后人继续探讨. ——译者注.

3,2 $\stackrel{2}{=}$ 7,6,4,1 作为生成子,我们将有 24 种结合方式,使各项平方之和等于逆序数的平方之和. 其中的两个例子是 87,56,34,21 $\stackrel{2}{=}$ 12,43,65,78;以及 86,54,31,27 $\stackrel{2}{=}$ 72,13,45,68.

如果其中个别生成子为 0,关系式仍有可能成立. 例如 1,3,5,9 $\stackrel{2}{=}$ 4,6,8,0,由此出发仍可导出 24 个等式,其中之一是 10,54,96,38 $\stackrel{2}{=}$ 01,45,69,83. 甚至从人们已经非常熟悉的关系 $3^2+4^2=5^2+0^2$ 也能导出 $35^2+40^2=04^2+53^2$ 或 $30^2+45^2=54^2+03^2$.

此等关系的成立,来自下列事实:若

[163]

$$x_1^2+x_2^2+\cdots+x_n^2=y_1^2+y_2^2+\cdots+y_n^2$$

(其中有若干项可以为 0),则

$$(10x_1+y_1)^2+(10x_2+y_2)^2+\cdots+(10x_n+y_n)^2$$

必定等于

$$(10y_1+x_1)^2+(10y_2+x_2)^2+\cdots+(10y_n+x_n)^2,$$

即使 x 的项与 y 的项以任意方式调动都没有影响,因为书写生成系列各项时,孰先孰后都不会影响其和.

进到高次幂后,三度等幂和关系 1,4,5,5,6,9 $\stackrel{3}{=}$ 3,2,3,7,8,7 可以作为 $6!=720$ 个等式的生成子,其中之一是 13,42,53,57,68,97 $\stackrel{3}{=}$ 79,86,75,35,24,31.

借助于更为复杂的生成子,我们可以得到具有良好逆序特性的由三位数或四位数组成的三度等幂和关系. 例如:132,223,241,243,312,314,332,423 $\stackrel{3}{=}$ 324,233,413,213,342,142,322,231;以及 1234,2455,2565,3346,4541,5322,5432,6653 $\stackrel{3}{=}$ 3566,2345,2235,1454,6433,5652,5542,4321.

通过数字偶的帮助,我们甚至能够得到回文数(顺读、倒读

都一样)的等幂和关系式. 例如 13031,42024,53035,57075,68086,97079 $\stackrel{3}{=}$ 31013,24042,35053,75057,86068,79097. 其中的每一项全都是回文数.

从生成子 1,5,6 $\stackrel{2}{=}$ 2,3,7 与 2,4,9 $\stackrel{2}{=}$ 1,6,8 出发,我们将得以完成回文二度等幂和关系式 1221,5445,6996 $\stackrel{2}{=}$ 2112,3663,7887. 再利用第三个生成子 2,2,5 $\stackrel{2}{=}$ 1,4,4 并与前两者相结合,我们即可得出六位回文二度等幂和关系 122221,542245,695596 $\stackrel{2}{=}$ 211112,364463,784487. 还有一个七位回文三度等幂和关系十分奇怪,但此时有些相邻的二位数码要看作一个整体那样对待,这个怪异的式子是:1030301,6030306,$\overline{6}\overline{13}\overline{13}\overline{06}$,$\overline{11}\overline{13}\overline{13}\overline{11}$ $\stackrel{3}{=}$ 3010103,2070702,$\overline{10}\overline{09}\overline{09}\overline{10}$,$\overline{9}\overline{15}\overline{15}\overline{09}$ $\stackrel{3}{=}$ 2010102,3090903,9070709,$\overline{10}\overline{15}\overline{15}\overline{10}$. 上面划线的二个数字是要当作一个整体的.①

高次等幂和关系式中,其各项也可以是"多角形数"与各种"棱锥数"(请参阅第 18 章). 前面已讲过,三角形数是多角形数之一,其形式为 $n(n+1)/2$. 例如在 $n=1,19,28$ 时可得出相应的三角形数 1,190,406. 这些三角形数再添上几个之后,即可得出三度等幂和关系 1,190,406,1770,2145,4095,5353 $\stackrel{3}{=}$ 3,105,780,1035,2926,3655,5356. 三角形数的一个四度等幂和关系为 1,325,496,3570,3828,9045,12561,16653,19701 $\stackrel{4}{=}$ 3,171,903,2211,6441,6786,14365,15400,19900. 甚至七度等幂的关〔164〕系也都找到了.

有时,多度等幂和关系中的各项 n,指的是第 n 个三角形数,而不是指通常的第 n 个自然数. 例如在 1,4,6,7 $\stackrel{2}{=}$ 2,3,5,8

① 原文如此. 作者说漏了嘴,其实此式是七位数与八位数都有的混合部队. ——译者注.

中，我们按三角形数的通项公式 $n(n+1)/2$ 分别代入，即得 1，10，21，28＝3，6，15，36. 另一个例子是 5，8，10，11 $\stackrel{2}{=}$ 6，7，9，12，它所对应的三角形数为 15，36，55，66＝21，28，45，78. 如果把这两个式子相加，还可得到 6，12，16，18 $\stackrel{2}{=}$ 8，10，14，20，它也有类似性质. 如果用记号 2，T 表示具有三角形数性质的二度等幂和关系，上面的最后一式其实应记为 6，12，16，18 $\stackrel{2,T}{=}$ 8，10，14，20. 此时，相应三角形数之和为 406.

如果我们分别用记号 S_1，S_2，S_T 来表示(1) 等幂和关系式各数之代数和；(2) 它们各自平方后的代数和；(3) 相应三角形数之代数和，则可得出神奇的关系式 $1-2-3+4 \stackrel{2,T}{=} 5-6-7+8 \stackrel{2,T}{=} 9-10-11+12=\cdots$，这里，$S_1=0$，$S_2=4$，$S_T=2$.

* * *

利用这些等式还可以做许多表演. 在 123789，561945，642864 $\stackrel{2}{=}$ 242868，323787，761943 中，砍掉各数的第一位数码后，所余之等式，对一次方与二次方依然成立，即 23789，61945，42864 $\stackrel{2}{=}$ 42868，23787，61943. 此种过程可以逐步施行下去，每次砍掉一个数码，直至最后各项只剩一位，此时仍有 9，5，4 $\stackrel{2}{=}$ 8，7，3. 我们也可换一种砍法，先删去末位数，得 12378，56194，64286 $\stackrel{2}{=}$ 24286，32378，76194，这样从右面一一砍去，直到最后的 1，5，6 $\stackrel{2}{=}$ 2，3，7.

我们竟然也能同时砍去第二与第三位数码而得 1789，5945，6864 $\stackrel{2}{=}$ 2868，3787，7943. 在此结果中又同时砍去新的第二、三位数码，而最后得出等式 19，55，64 $\stackrel{2}{=}$ 28，37，73.

在找到此种神奇关系时所表现出来的聪明才智，看来似乎源远流长，尚未到达尽头. 拉丁格言真是说对了："生命短暂，艺术长存."

参考文献

Ball, W. W. R. *Mathematical Recreations and Essays.* New York: Macmillan Co., 1939.

Barlow, P. *Tables of Squares, Cubes, etc.* Chicago: Charles T. Powner Co., 1948.

[165]

——. *Theory of Numbers.* London: J. Johnson & Co., 1811.

Bastien, L. "[Congruent Numbers]," *L'Intermédiaire des Mathématiciens*, **22**(1915), 231.

Collins, M. "A Tract on the Possible and Impossible Cases of Quadratic Duplicate Equalities in the Diophantine Analysis," *British Association for the Advancement of Science*, **25** (1855), Notes and Abstracts, 2.

Cunningham, A. "On Finding Factors," *Messenger of Mathematics*, **20**(1890), 37.

Dickson, L. E. *History of the Theory of Numbers.* 3 vols. New York: Chelsea Publishing Co., 1950.

Draughton, H. W. "Solution to Problems: Find Nine Integral Numbers in Arithmetic Progression the Sum of Whose Squares Is a Square; Find Nine In tegral Square Numbers Whose Sum Is a Square," *American Mathematical Monthly*, **2**(1895), 129.

Gérardin, A. "[Congruent Numbers]," *L'Intermédiaire des Mathématiciens*, **22**(1915), 52.

Gloden, A. "Multigrade Prime-Number Identities," *Scripta Mathematica*, **16**(1950), 125.

——. "On Piza's Bigrades," *Scripta Mathematica*, **21**(1955), 193.

——. "Remarkable Multigrades," *Scripta Mathematica*, **21**

(1955),200.

Goldberg, M. "The Squaring of Developable Surfaces," *Scripta Mathematica*, **18**(1952),17.

Goormaghtigh, R. "Identities with Digits in Reversed Order," *Scripta Mathematica*, **17**(1951),19.

Hart, D. S. "Consecutive Square Numbers Whose Sum Is a Square," *Mathematical Magazine*, **1**(1883),119.

Heath, R. V. "Sums Equal to Products," *Scripta Mathematica*, **9**(1943),190.

——. "Bigrade Identities with a Special Condition," *Scripta Mathematica*, **18**(1952),68.

Hollcraft, T. R. "On Sums of Powers of *n* Consecutive Integers," *Bulletin of the American Mathematical Society*, **59** (1953),526.

Iyer, R. V. "Multigrades with Palindromic Numbers as Elements," *Scripta Mathematica*, **20**(1954),220.

Kaprekar, D. R., and Iyer, R. V. "Identities with Digits in Reversed Order," *Scripta Mathematica*, **16**(1950),160.

——. "Reversible Tarry-Escott Identities," *Scripta Mathematica*, **17**(1951),146.

Khatri, M. N. "'Graphs' of Identities," *Scripta Mathematica*, **21**(1955),202.

Kraitchik, M. *Recherches sur la Théorie des Nombres*. Vol. I. Paris: Gauthier-Villars et Cie., 1924.

Lehmer, D. N. *Factor Tables for the First Ten Million*. New York: Hafner Publishing Co., 1956.

Loyd, S. *Cyclopedia of Puzzles*. New York: Lamb Publishing Co., 1914.

Marenholz, M. "Mathematical Quintuplets," *Scripta Mathe-*

matica, **7**(1940), 159. [166]

Martin, A. "Some Curious Properties of Numbers," *Mathematical Magazine*, **1**(1883), 69.

Moessner, A. "Curious Identities," *Scripta Mathematica*, **6** (1939), 180.

——. "Arithmetic Operations on Multigrade Identities," *Scripta Mathematica*, **19**(1953), 282.

Piza, P. A. "Sums of Powers of Triangular Numbers," *Scripta Mathematica*, **16**(1950), 127.

——. "Telescoped Identities," *Scripta Mathematica*, **21** (1955), 90.

Steinhaus, H. *Mathematical Snapshots*. New York: Oxford University Press, 1960.

Stone, A. H., *et al*. "Problem for Solution: [Fitting Together Twenty-eight Squares to Form a Square]," *American Mathematical Monthly*, **47**(1940), 48.

——. "Solution to Problem: [Fitting Together Twenty-eight Squares to Form a Square]," *American Mathematical Monthly*, **47**(1940), 570.

Thebault, V. "Number Pleasantries," *Scripta Mathematica*, **12**(1946), 218.

White, W. F. *Scrap Book of Elementary Mathematics*. Chicago: Open Court Publishing Co., 1910. [167]

第16章 法莱数列

第10章里已讲过十进分数的一些性质了.可是一般分数也有不少有趣的性质.也许你回想得起,算术里头的普通分数是指分母、分子均为整数的那样一种分数.当分母大于分子时,该分数称为真分数.

如果指定一个分母的上限,再把各普通分数(以最简分数形式出现)按从小到大的次序排列,譬如说,当分母不大于7时,我们可以得出以下17个分数:$\frac{1}{7}$,$\frac{1}{6}$,$\frac{1}{5}$,$\frac{1}{4}$,$\frac{2}{7}$,$\frac{1}{3}$,$\frac{2}{5}$,$\frac{3}{7}$,$\frac{1}{2}$,$\frac{4}{7}$,$\frac{3}{5}$,$\frac{2}{3}$,$\frac{5}{7}$,$\frac{3}{4}$,$\frac{4}{5}$,$\frac{5}{6}$,$\frac{6}{7}$,这就是所谓的法莱数列.

约翰·法莱(John Farey)是生活在拿破仑时代的一位多才多艺之士.作为土地丈量与勘察人员的他,收集过不少化石与矿物,业余时间他在著名的《哲学杂志》上写了大量科普文章,题材散布之广令人惊讶.他真是一位"杂家",文章内容涉及地质,音乐,十进制钱币,马车轮盘,彗星,乃至本章要讲的法莱数列.他并不认为这个发现特别重要,更未预料到由于他发现了漏过机敏的费马与欧拉眼睛的一些小东西而使他得以在数学中名垂青史.然而必须遗憾地指出,数学里头一再发生这类事情:享有盛名者并非原始发现人.有个名叫哈罗斯(C. Haros)的人比法莱的发现早14年,但大数学家柯西不知道此事,而把功劳归在法莱名下,其他的人则重复了柯西的说法.看来,法莱的运气较好,"法莱数列"发起音来要比"哈罗斯数列"好听一些.也许有某个

阿拉伯数学家比哈罗斯的发现还要早上一千年，真是天晓得！

这些事实在1816年（约翰·法莱在这一年首次观察到）之前从未有人研究过，这种说法真令人不敢相信. 发现是在仔细审阅亨利·戈德温所编的、冗长的小数商表格时作出的，本书第10章已讲过戈德温其人. 法莱的意外发现马上被当时的数学家们紧紧抓住，不久以后，此种分数的理论即被彻底阐明. 其中的部分理论是相当粗浅的，而另一些则比较深奥一些，此种情况，对号称“数学女王”的数论来说，并不鲜见. [168]

在注视上述数列时马上会产生一些问题：

1. 这种分数究竟有多少？其个数能否表示为给定数（例如上例中的分母7）的函数？

2. 相邻分数之间有何种联系？

只要对数列略瞥一眼，即可回答第二个问题. 对相邻的三个分数而言，中间分数的分子是左、右两个分数的分子相加而得，分母也类似. 当然所得之结果尚需约分，化成最简分数. 例如在上述数列中可任取毗邻的三项$\frac{3}{5}$，$\frac{2}{3}$，$\frac{5}{7}$，于是得到$\frac{3+5}{7+5}=\frac{8}{12}=\frac{2}{3}$. 循此规则，只要给出数列的前两项，即可推出相继各项. 而对前两项来说，如果分母不准超过7，当然肯定是$\frac{1}{7}$与$\frac{1}{6}$. 设第三个分数为$\frac{x}{y}$，于是$\frac{1}{7}$，$\frac{1}{6}$，$\frac{x}{y}$形成一个三数组. 根据上述法则，$\frac{1+x}{7+y}=\frac{1}{6}$，当然这不一定意味着$1+x=1$，$7+y=6$，因为$\frac{1}{6}$也可通过约分而来. 但若$z$为分子、分母的最大公因子，则

$$1+x=z\cdot 1,$$
$$7+y=z\cdot 6.$$

从而$x=z-1$，$y=6z-7$. 由于y不能超过7，z只能是2，于是$x=1$，$y=5$，故第三个分数是$\frac{1}{5}$. 对三数组$\frac{1}{3}$，$\frac{2}{5}$，$\frac{x}{y}$来说，我们

有 $1+x=2z$，$3+y=5z$，即 $x=2z-1$，$y=5z-3$. 这时 z 的可能值是 1 或 2，而 $z=2$ 是唯一的正确值. 有一个规则可解决模棱两可的迷惑.

设 n 为法莱数列之阶（就上例而言，$n=7$），且 $\frac{a}{b}$，$\frac{a'}{b'}$，$\frac{x}{y}$ 是数列中相邻的三项，则 $a+x=za'$，$b+y=zb'$，这里的 z 是等于或小于 $(n+b)/b'$ 的最大整数. 显然，等于或小于 $\frac{7+3}{5}$ 的最大整数是 2. 对三数组 $\frac{1}{7}$，$\frac{1}{6}$，$\frac{x}{y}$ 的前一例来说，我们有 $z\leqslant(7+7)/6$，亦即 $z=2$.

在取三数组 $\frac{5}{7}$，$\frac{3}{4}$，$\frac{x}{y}$ 时，则有 $z\leqslant\frac{7+7}{4}$，因而 $z=3$，于是 $5+x=3\cdot3$，$7+y=3\cdot4$，故得出 $x=4$，$y=5$. 这就求出接在 $\frac{3}{4}$ [169] 后面的分数 $\frac{4}{5}$ 了.

阶为 n 的法莱分数的个数可由下法求得：既然所有的分数均为最简分数，对给定分母 b 来说，分子的个数必定是小于 b 且与之互质的诸数之和，即欧拉函数 $\phi(b)$. 对从 2 到 n 的一切正整数均可援用此种推理法，因此，阶为 n 的法莱分数的个数 N 应当等于 $\phi(2)+\phi(3)+\phi(4)+\cdots+\phi(n)$. 若 $n=7$，我们即有

$$\begin{aligned} N &= \phi(2)+\phi(3)+\phi(4)+\phi(5)+\phi(6)+\phi(7) \\ &= 1+2+2+4+2+6=17. \end{aligned}$$

n 增大时，N 的值随之迅速递增，$n=100$ 时，$N=3043$. 由此可知，分子与分母都不超过 100 时，竟有如此之多的既约普通分数.

读者们也许想证明法莱数列中相邻三数之间分子、分母所存在的关系以及上述求 z 的规则. 这里要告诉读者，证明并不太容易.

法莱数列的另一性质是：与$\frac{1}{2}$等距离的两个分数是互补的，其和等于1．除$x=1$与$x=2$外，$\phi(x)$恒为偶数．因此

$$N=\phi(2)+\phi(3)+\cdots+\phi(n)$$

恒为奇数．因此法莱数列的项数必定是奇数，而其正中的一项必为$\frac{1}{2}$．

还有一个性质：相邻两个分数之差一定等于它们的分母乘积之倒数．

* * *

在ϕ函数与常数π（即圆周率，圆的周长与直径之比）之间存在着奇妙的联系．事实上，和式

$$\phi(1)+\phi(2)+\phi(3)+\cdots+\phi(n)$$

近似于$3n^2/\pi^2$，当n增大时，近似程度越来越好．第一项是可以忽略不计的，弃去它不会显著影响其结果，这样一来上面的和式便是阶为n的法莱数列的项数N了．由于我们已经算出π的很多位小数（已算出π的100000位小数）[1]，这就意味着我们可以大致估计出一个法莱数列有多少项，而不必去一一计算$\phi(1)$，$\phi(2)$，$\phi(3)$，…，$\phi(n)$． [170]

例如$n=100$时，我们将有

$$N=(3\cdot 100^2)/\pi^2=3039.6355\cdots,$$

而确切的数值是3043．

大数学家西尔维斯特(J. J. Sylvester)算出分母不超过n（n的范围为1到500）的法莱数列的项数N，并把它拿来同$3n^2/\pi^2$比较．由于正确程度随n的递增而变得更好，摘录在下面的他的

[1] 此处的数据已大大过时，目前已知的记录是π已被算到小数点后43亿位．——译者注．

表格也许是能使读者感到兴趣的.

n	$\phi(n)$	$N=\Sigma\phi(n)-1=$ $\phi(2)+\phi(3)+\cdots+\phi(n)$	$3n^2/\pi^2$
1	1	0	0.30
2	1	1	1.22
3	2	3	2.74
4	2	5	4.86
5	4	9	7.60
6	2	11	10.94
7	6	17	14.90
8	4	21	19.46
9	6	27	24.62
10	4	31	30.40
15	8	71	68.39
25	20	199	189.98
50	20	773	759.91
100	40	3043	3039.64
200	80	12231	12158.54
300	80	27397	27356.72
400	160	48677	48634.17
500	200	76115	75990.89

表 71 法莱数列的项数

研究家们又从法莱数列导出了其他许多数列,并用很多篇幅探讨了它们的性质.

参考文献

Bell, E. T. *The Last Problem*. New York: Simon and Schuster, 1961.

Dickson, L. E. *History of the Theory of Numbers*. 3 vols. [171] New York: Chelsea Publishing Co., 1950.

Farey, J. "On a Curious Property of Vulgar Fractions," *London, Edinburgh and Dublin Philosophical Magazine*, **47** (1816), 385.

Glaisher, J. W. L. "On a Property of Vulgar Fractions," *London, Edinburgh and Dublin Philosophical Magazine* (Fifth Series), **7**(1879), 321.

Hardy, G. H. "An Introduction to the Theory of Numbers," *Bulletin of the American Mathematical Society*, **35**(1929), 778.

Shanks, D., and Wrench. J. W., Jr. "Calculation of π to 100,000 Decimals," *Mathematics of Computation*, **16**(1962), 76.

Sylvester, J. J. "On the Number of Fractions Contained in Any Farey Series of Which the Limiting Number Is Given," *London, Edinburgh and Dublin Philosophical Magazine* (Fifth Series), **15**(1883), 251. [172]

第17章 等分圆周

数学的一大魅力在于：全然无关的领域竟能以出人意外的方式彼此联系. 谁会想到，数论竟能用来确定哪些圆内接正多边形可以用尺规作图，哪些则不可能. 曾经探讨过形为 $2^{2^n}+1$ 的正整数的费马(后人将这类数称为“费马数”)不曾想到这一理论与内接正多边形有着密切联系，只有睿智的高斯才能发现.

并不是费马认为他已证明了的东西遭到了否定. 他对费马数仅不过提了一种看法，而且他曾说过他未能找到令人满意的证法. 他认为 $2^{2^n}+1$ 将永远给出素数，而事实上现能确证的仅有 $n=0,1,2,3,4$ 这些值，与之对应的素数为 3，5，17，257，65537. 但当 $n=5$ 时，费马数 F_5 具有因子 641 与 6700417，以费马之天才(他能对诸如 100895598169 这类大数分解因子，就像一位魔术师在帽子里变出兔子那样轻松)居然会漏掉 F_5 中的一个很小的因子 641，真教人惊讶. 对于那些难以抗拒强烈诱惑，想从数据而不是通过严格证明来得出结论的业余研究家来说，再也没有比一位天才的失败更强的告诫了. 使费马的错误结论更严重的是，迄今为止，对 n 大于 4 的每一个费马数 F_n，验证下来全是合数，这就令人有理由怀疑，是否其结论的对立面是对的？或许以后会有人证明，仅当 n 小于 5 时，F_n 才是一个素数.

641 确是 $2^{32}+1$ 的一个除数，这很容易从同余式推出，但当费马思索这些问题时，发明同余式理论的高斯却还没有出生呢.

如果没有该理论，当n的数值很大时，验证可除性简直是根本不可能的. [173]

像

$$F_{73}=2^{2^{73}}+1$$

（此数有一个因子已被析出）这样的庞然大物，要具体掌握其大小颇为不易. 此数如此之大，若用常规编排方式，则全世界所有图书馆的全部书籍都将容纳不下它. 此断言并非夸下海口，不难证明其正确性. 由于 $2^{10}=1024$ 大致上相当于 $10^3=1000$，不妨近似地当它是一千. 于是 $2^{70}=10^{21}$，而 2^{73}接近于 10^{22}. 从而 F_{73}大致上相当于 $2^{10^{22}}=2^{10\cdot10^{21}}$，由于 2^{10}接近于 10^3，故有 $2^{10\cdot10^{21}}=(10^3)^{10^{21}}=10^{3\cdot10^{21}}$，所以 F_{73}大约有 $3\cdot10^{21}$位数码. 现在假定世上每本书有 1000 页，而每页有 100 行，每行有 100 个字母或数码，实际上这已远远超过每本书的平均信息容量. 又设世上有一百万家图书馆，每家藏书一亿册，于是，这些书中所含字母或数码将是 $1000\cdot100\cdot100\cdot1,000,000\cdot100,000,000=10^{21}$，而 F_{73}中所含的数码个数将是它的三倍之多！

也可用其他办法来估算. 设每个数码有 1 毫米见方，则满载全部数码的这一行将长达 $2700\cdot10^{12}$千米，将可环绕地球赤道 600 亿次. 假定有人用 1 秒钟写下一个数码，他每天工作 10 小时，一年干 360 天，则把全部数码写下来，需要 230 亿年！如果世上全部人口（据估计为 32 亿，即 $3.2\cdot10^9$ 人[①]）都来从事这一工作，也将要 82000 年之久！若每个数码占地 1 平方毫米，则需要地球表面积的五倍才写得下这个数.

即便是小得多的 F_{36}也超过 200 亿（$20\cdot10^9$）位.

附表 72 给出了截止 1961 年的费马数的因子.

*　　　*　　　*

① 此数据是从前的估计，现在，世界上约有 55 亿人口. ——译者注.

[175]

n	性质	以乘幂形式给出的因子	以整数形式给出的因子
0	素数	—	3
1	素数	—	5
2	素数	—	17
3	素数	—	257
4	素数	—	65537
5	合数	$(2^7\cdot5+1)(2^7\cdot52347+1)$	641 • 6700417 *
6	合数	$(2^8\cdot3^2\cdot7\cdot17+1)(2^8\cdot5\cdot52562829149+1)$	274177 • 67280421310721 *
7	合数	有 2 或 3 个因子，全都大于 2^{32}	(?)
8	合数	(?)	(?)
9	合数	$(2^{16}\cdot37+1)\cdot(?)$	2424833 • (?)
10	合数	$(2^{12}\cdot11131+1)\cdot(?)$	45592577 • (?)
11	合数	$(2^{13}\cdot3\cdot13+1)(2^{13}\cdot7\cdot17+1)\cdot(?)$	319489 • 974849 • (?)
12	合数	$(2^{14}\cdot7+1)(2^{16}\cdot397+1)(2^{16}\cdot7\cdot139+1)\cdot(?)$	114689 • 26017793 • 63766529 • (?)
13	合数	合数，所有因子不小于 2^{35}，素因子个数不明.	(?)
15	合数	$(2^{21}\cdot3\cdot193+1)\cdot(?)$	1214251009 • (?)
16	合数	$(2^{19}\cdot1575+1)\cdot(?)$	825753601 • (?)
18	合数	$(2^{20}\cdot13+1)\cdot(?)$	13631489 • (?)
23	合数	$(2^{25}\cdot5+1)\cdot(?)$	167772161 • (?)
36	合数	$(2^{39}\cdot5+1)\cdot(?)$	2748779069441 • (?)
38	合数	$(2^{41}\cdot3+1)\cdot(?)$	6597069766657 • (?)
73	合数	$(2^{75}\cdot5+1)\cdot(?)$	188894559314785808547841 • (?)

* 已完全分解.

表 72①　费马数 $F_n=2^{2^n}+1$ 的素因子

① 本书下次重印时，表 72 将予修订. ——原注.

早在 1770 年，晚年盲目的数学家欧拉已证明，当 a，b 互质时，$a^{2^n}+b^{2^n}$ 的任一因子要么是 2，要么具有 $2^{n+1}K+1$ 的形状. 费马数是这个一般定理的特例，因此时可视为 $a=2$，$b=1$. 一百多年之后，卢卡在 1878 年证明了，$2^{2^n}+1$ 的每一个素因子都必然具有 $2^{n+2}L+1$ 的形式. 就附表 72 而言，F_5 的一个因子 641 即等于 $2^{5+2}\cdot 5+1$，而另一因子 $6700417=2^{5+2}\cdot 52347+1$. 对 $F_7=2^{2^7}+1$ 而言，已知它为合数但因子不明，然而其素数因子必具有 $2^9\cdot K+1$ 的形式；而 $F_8=2^{2^8}+1$ 的除数形式为 $2^{10}\cdot K+1$. 另外，也已知道当且仅当 $3^{\frac{F_n-1}{2}}\equiv -1 \bmod F_n$ 时，F_n 为素数. [174]

* * *

费马数自身值得注意，它们还有显著的几何应用，在论述之前复习一下初等几何颇有帮助. 绝大多数读者也许已经知道怎样等分一线段或一圆弧. 显然，用这种反复进行二等分的办法，可把一圆弧等分为 2，4，8，…，2^n 等分. 人们也回想得起，除了 90°的整数倍以及少数几个 90°的分数之外，不可能用圆规与直尺三等分一角；实际上，角的三等分问题一直是许多世纪以来像鬼火一样捉摸不定的东西.

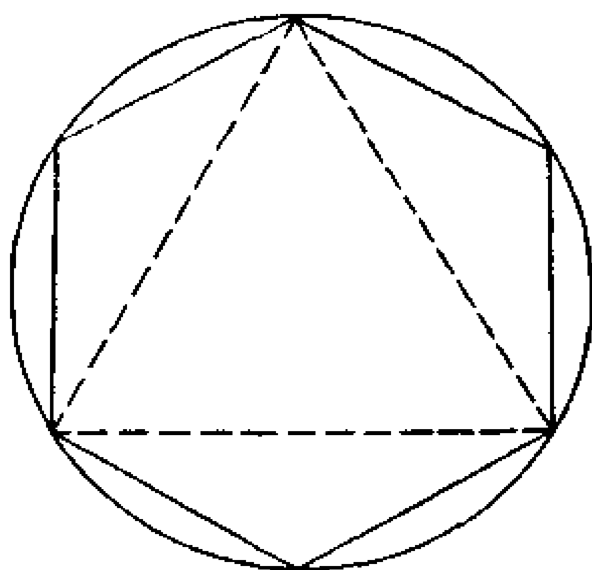


图 9 内接正三角形与正六边形 [176]

圆内接正六边形极易作出，只要像图 9 那样，用半径作为弦，在圆周上相继截取六次；把六边形相间的顶点连结起来，即可得到内接正三角形.

依次连结两条互相垂直的直径的端点即可得出内接正方形. 对图 9 中的圆弧反复二等分，即可作出正 12，正 24，正 48，……，正 $2^n \cdot 3$ 边形. 与此相仿，从内接正方形出发，可以得出正八边形……以及任意正 2^n 边形.

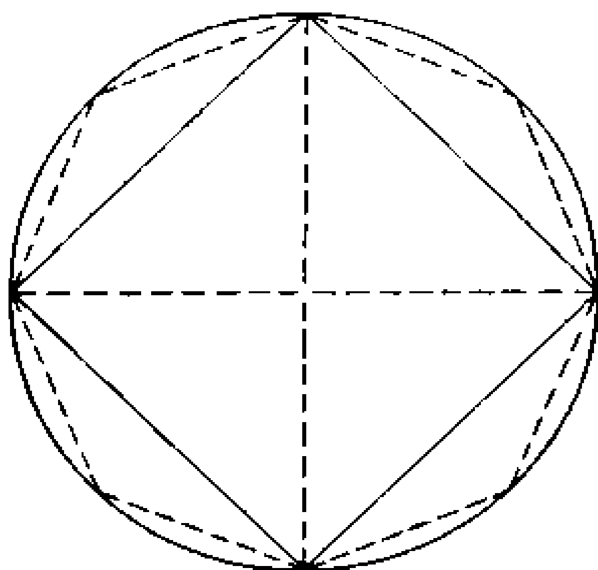


图 10 内接正方形与正八边形

初等几何中正五边形的尺规作图法或许读者也能回忆得起. 作法如下：在单位圆（见附图 11）中，AC 与 BD 是互为垂直的直径，E 为 AO 之中点，而 $EF = EB$.

以 B 为圆心，BF 为半径作弧，截圆周于点 G，则 BG 即为正五边形之一边. 此种作法之详细证明在大多数几何书里都能找到.

随后的讨论中将提到，线段可用来表示含有二次根式的代数式，正五边形每边之长即为其中之一. 易证 $(BG)^2$ 等于 $(5-\sqrt{5})/2$. 由于 $BO=1$（单位圆的半径），$EO=\frac{1}{2}$，从而 $EB=$

图 11 内接正五边形之作法

[177]

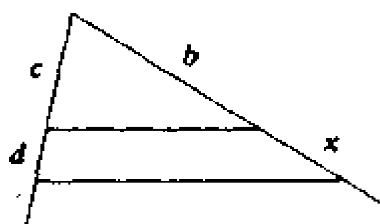
$\sqrt{1+\frac{1}{4}}=\sqrt{5}/2, EF=\sqrt{5}/2, OF=\sqrt{5}/2-1/2$，故$(BG)^2=(BF)^2$（是指线段而不是弧）$=(BO)^2+(OF)^2=1+(\sqrt{5}/2-1/2)^2=(5-\sqrt{5})/2$.

因此用直尺和圆规可以作出正 $2^n\cdot 5$ 多边形. 然而，尽管我们反复试验多次，却依然未能利用这些工具作出圆内接正七边形或正九边形.

由于可作出圆内接正三角形及正五边形，而 3 与 5 又是互质数，因而圆内接正 15 边形以及任何正 $2^n\cdot 15$ 边形也都可作. 在第 5 章中已讲过，对任意两个给定的互质数 p,q，一定可以找到另外两数 a,b，以使得 $pa-qb=1$，从而有$\frac{a}{q}-\frac{b}{p}=\frac{1}{pq}$. 若 5 与 3 是给定的正整数，则 $a=2,b=3$，且有$\frac{2}{3}-\frac{3}{5}=\frac{1}{15}$. 于是，只要

圆内接正五边形与内接正三角形已经作好，则由正三角形一边所张弧的二倍减去正五边形所张弧的三倍，其差即等于圆周长的$\frac{1}{15}$.

到此地步，也不妨看一看，积与商是怎样通过几何手段作出的. 代数式 db/c 很易作出，因若令 $db/c=x$，则有 $c/d=b/x$. 我们像图 12 那样作两条相交直线，并从交点开始，在一条直线上分别截取线段 c 与 d，在另一直线上截取线段 b，连结 c 与 b 之端点作一直线，并通过 d 之端点作一直线与之平行，这样，所要求的线段 x 即可得出.



[178]

图 12 求第四比例项

有时候，问题中的某个量是经过乔装的. 例如有这样的作图题：给定线段 m，n 的长度，求积 mn. 这时，要任取一个单位长线段，于是即得

$$mn/1=x,\ 即\ 1/m=n/x.$$

然后照上面所讲的办法，截取线段 1，m，n 并由此而求得 x.

如果想作出 $\sqrt{pq}$，由于 $x^2=pq$，所以 x 是 p 与 q 的比例中项. 这时可以先截取线段，使其长分别等于 p 与 q(见图 13)，然后以它们的和为直径作一个半圆，并在 p，q 之连接点处作一垂线，并与半圆交于一点. 垂线的这一段即为所要求的 x. 如果只要作出 $\sqrt{p}$，我们可把它解释为 $x=\sqrt{p\cdot 1}$，即 $x^2=p\cdot 1$. 在取好单位长与线段 p 之后，仍可像上面那样，把 x 求出来.

更为复杂的表达式，例如$\sqrt{p+\sqrt{pq}+r-\sqrt{s}}$也可类似地

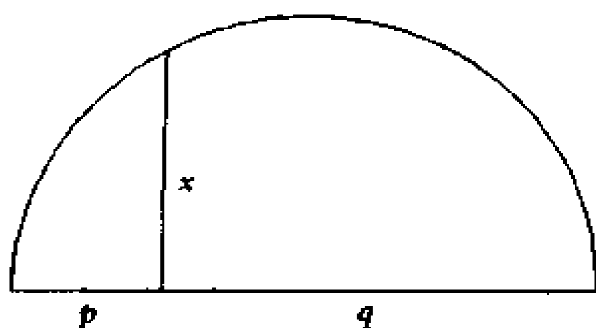


图 13 求比例中项

用直尺、圆规作出. 例如,在单位圆中,内接正五边形的一边之长等于$\sqrt{(5-\sqrt{5})/2}$,图 11 的作法表明,线段 BG 之长便是这一代数式的几何等价物.

我们现在已经作好准备,可以追随高斯的辉煌而深入的推理. 他已证明,圆内接正多边形的尺规作图,仅在以下几种情况才有可能:(1)正多边形之边数为 $2^{2^n}+1$ 形式的素数;(2)此类素数(全是不同的)的乘积;(3)2 的乘幂与一个或多个上述形式的素数之乘积. 边数为 2^n;$2^n \cdot 3$;$2^n \cdot 5$;$2^n \cdot 15$ 的正多边形的作图在希腊时代即已知晓,但在高斯之前,世上没有任何人会想到在上述这些正多边形之外,还有其他正多边形也可用尺规作出. 这条崎岖小路是由代数学里许多定理铺筑起来的. [179]

导致高斯作出结论的,大致有以下一些步骤(已作出相当简化):

1. 如果一个数量能通过有限次的二次根式来表达,则它可以由尺规作出. 例如

$$x=\left[\sqrt{a+\sqrt{c+ef}}+\sqrt{d+\sqrt{b}}\right]\Big/(\sqrt{a}+\sqrt{b})+(p+\sqrt{q})\Big/\sqrt{r}$$

就可以作出.

2. 存在着以这样一些数量为其解(根)的方程,对于给定的

不等根来说，只有唯一的次数为最低的方程能为这些根所满足．这一个次数最低的方程称为既约方程，因为它已不再能分解为两个或两个以上未知数的幂指数为整数的因子．

3．由含有有限多个二次根式所表示的量满足的既约方程的次数永远是 2 的乘幂，如果一个既约方程不是 2^n 次的，则其解不可能是仅含有限多个二次根式的代数式．

4．二项方程 $x^n-1=0$ 的根，在两条互相正交的轴所构成的平面坐标系（其中之一为实轴；上面的点表示实数，另一为虚轴，上面的点表示虚数）中作图时，这些根所表示的点必然等距地分布在一个单位圆的圆周上，此圆的圆心是两轴之交点，而半径为 1 个单位．

5．对某个合数 $n=pq$，方程 $x^n-1=0$ 的根可用尺规作出，如果 $x^p-1=0$ 与 $x^q-1=0$ 的根也能用尺规作图的话．因为 $n=pq$，n 是两个互质数的乘积，所以一定可以找出两个整数 a、b，以使得 $ap-bq=1$ 或 $a/q-b/p=1/qp$，从而圆周可以等分成 pq 份．由此可知，在考虑圆周长能否分作 n 等分时，只要考虑 n 是素数或素数的乘幂就已足够．

6．由于我们已经知道怎样用尺规等分一段圆弧，而这种作图法可以反复进行，因此圆周可以分成 $2,4,8,\cdots,2^a$ 个等分．从而可推知，如果我们能把圆周分成 n 等分（n 是奇数，素数或合数）的话，我们也就能把它分成 $2^a\cdot n$ 个等分．

[180] 7．如果我们把方程 $x^p-1=0$（此处 p 是素数）用相当于唯一实根 $x=1$ 的因子 $x-1$ 去除，即可得出

$$(x^p-1)/(x-1)=x^{p-1}+x^{p-2}+x^{p-3}+\cdots+1=0,$$

它的根便是原方程的复数根．此方程名为分圆方程，是既约方程，它的根都在单位圆的圆周上．

8．由于分圆方程是既约方程，仅当它的次数为 2^h 时，才能通过二次根式求解，亦即 $p-1=2^h$，或 $p=2^h+1$．

9. 为使 $p=2^h+1$ 是一素数，h 必须是 2 的 2^n 方次幂，否则 h 至少会有一个奇数因子 e，使 $h=ef$，而 $p=2^h+1=(2^f)^e+1$，而后者将恒有一个 2^f+1 的因子，从而决不是一个素数了.

10. 仅当 n 取下列形式

$$2^{a_0}(2^{2^{a_1}}+1)(2^{2^{a_2}}+1)\cdots(2^{2^{a_n}}+1)$$

时，圆周才能用尺规分成 n 个等分. 这里，每个括弧都是素数的一次方幂，而 $a_1,a_2,\cdots,a_n$ 都是不同正整数.

由表 72 可知，形如 $2^{2^n}+1$ 中的数而为素数者仅有 3;5;17;257 与 65537;因而，从理论上讲，可以用尺规作图法作出的正多边形的个数只能是以上五个整数取法的排列组合，即 $2^5-1=31$ 种. 这些正多边形的边数如表 73 所示.

[181]

编号	多边形的边数
1	3 = 3
2	5 = 5
3	15 = 3 · 5
4	17 = 17
5	51 = 3 · 17
6	85 = 5 · 17
7	255 = 3 · 5 · 17
8	257 = 257
9	771 = 3 · 257
10	1285 = 5 · 257
11	3855 = 3 · 5 · 257
12	4369 = 17 · 257
13	13107 = 3 · 17 · 257
14	21845 = 5 · 17 · 257
15	65535 = 3 · 5 · 17 · 257
16	65537 = 65537
17	196611 = 3 · 65537
18	327685 = 5 · 65537
19	983055 = 3 · 5 · 65537
20	1114129 = 17 · 65537

表 73 拥有奇数条边，并能通过直尺与圆规作图的正多边形

编号	多边形的边数
21	$3342387 = 3 \cdot 17 \cdot 65537$
22	$5570645 = 5 \cdot 17 \cdot 65537$
23	$16711935 = 3 \cdot 5 \cdot 17 \cdot 65537$
24	$16843009 = 257 \cdot 65537$
25	$50529027 = 3 \cdot 257 \cdot 65537$
26	$84215045 = 5 \cdot 257 \cdot 65537$
27	$252645135 = 3 \cdot 5 \cdot 257 \cdot 65537$
28	$286331153 = 17 \cdot 257 \cdot 65537$
29	$858993459 = 3 \cdot 17 \cdot 257 \cdot 65537$
30	$1431655765 = 5 \cdot 17 \cdot 257 \cdot 65537$
31	$4294967295 = 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537$

表 73 拥有奇数条边,并能通过直尺与圆规作图的正多边形(续)

2 的任意次正整数幂均可以同上述 31 个数相结合以得出几何上可作的,且边数为偶数的正多边形;边数不超过 100 时,此类边数为奇数或偶数的正多边形是 24 个;不超过 300 时有 37 个;不超过 1000 时有 52 个,不超过一百万时则有 206 个.边数不超过 100 的 24 个正多边形见附表 74.

序号	边数	序号	边数
1	3	13	30
2	4	14	32
3	5	15	34
4	6	16	40
5	8	17	48
6	10	18	51
7	12	19	60
8	15	20	64
9	16	21	68
10	17	22	80
11	20	23	85
12	24	24	96

表 74 可以用尺规作图的正多边形

尽管从理论上说,边数由表 73 给出的正多边形均可以用尺规作出,但实际上做到这事却决非简单.即使对正 17 边形,分析

与作法已经相当复杂；对正 257 边形就需用去大量笔墨纸张. 林根 的海默斯(Hermes)教授为了作出正65537边形，足足消磨了他一生中的十年时光！ [182]

正 17 边形的一边可由下法求出(图 14)：

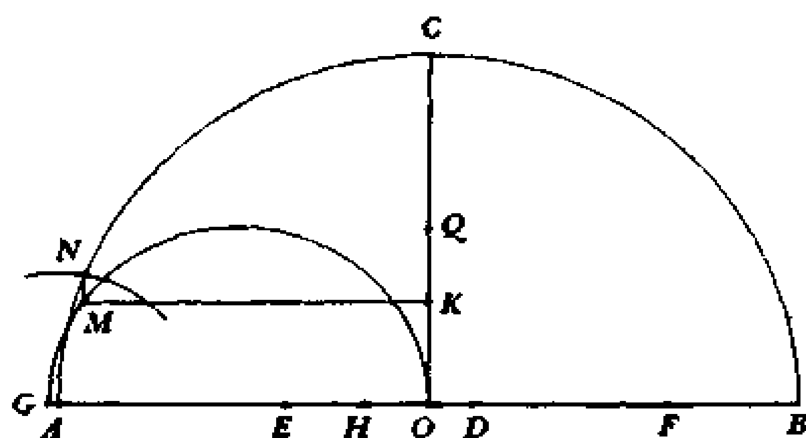


图 14 内接正十七边形的作法

在半圆的半径 OC 上求出中点 Q，并在垂直于该半径的直径上，自圆心 O 截取线段 OD，使它等于半径的$\frac{1}{8}$. 作 DF 与 DE，使它们都等于 DQ. 又作 EG 与 FH，使之分别等于 EQ，FQ. 再作OK，使它等于OH 与OQ 的比例中项. 过K 作 KM 平行于AB，而与罩住OG的半圆周相交于M，作MN平行于OC，与 O 圆相交于 N. 则弧$\overset{\frown}{AN}$就是圆周长的$\frac{1}{17}$. 这一作法是由一个名叫约翰·路利(John Lowry)的人在 1819 年给出的，他的证明在那一年的《数学博览》杂志上足足占去九页之多！ [183]

* * *

高斯对他所发现的费马素数与内接正多边形的关系极为自豪，念念不忘，因此他希望在他去世之后，在其墓碑上刻上一个正 17 边形. 由于种种原因，他的要求未获当局批准，但是在德国勃朗茨维格郡(他的出生地)的一个纪念碑上，的的确确刻上了正 17 边形.

* * *

对于寻找 $2^{2^n}+1$ 形的素数并不满足，数学家们又去研究 $10^{2^n}+1$，但是直到 $n=6$ 为止，迄今已找到的素数只有两个：11 与 101，相当于 $n=0$ 与 $n=1$ 的情形.

* * *

一度曾经猜想过 $2+1, 2^2+1, 2^{2^2}+1, 2^{2^{2^2}}+1$ 等全是素数，但是，后来发现 $2^{2^{16}}+1$ 是个合数，具有因子 $2^{19}\cdot 1575+1=825753601$. 在数论中，猜想经常是不可靠的.

参考文献

Ball, W. W. R. *Mathematical Recreations and Essays*. New York: Macmillan Co., 1939.

Carmichael, R. D. "Fermat Numbers $F_n=2^{2^n}+1$," *American Mathematical Monthly*, **26**(1919), 137.

Klein, F. *Famous Problems of Elementary Geometry*. New York: Dover Publications, Inc., 1956.

Kraitchik, M. *Recherches sur la Théorie des Nombres*. Paris: Gauthier-Villars et Cie., 1924.

Paxson, G. A. "The Compositeness of the Thirteenth Fermat Number," *Mathematics of Computation*, **15**(1961), 420.

Robinson, R. M. "Mersenne and Fermat Numbers," *Proceedings of the American Mathematical Society*, **5**(1954), 842.

Selfridge, J. L. "Factors of Fermat Numbers," *Mathematical Tables and Other Aids to Computation*, **7**(1953), 274.

Young, J. W. A. *Monographs on Topics of Modern Mathematics*. New York: Dover Publications, Inc., 1955.

[184]

第18章 球　戏

凡是去过保龄球场的人都知道，十只木瓶是按三角形方式摆放的."打落袋"桌球的人在不玩耍时也把15只球布置成三角形模式.碟子，木球，筹码以及诸如此类的小东西，凡是能配置成等边三角形模式的(见图15)，其数目称为三角形数.显然，它是从1开始的连续正整数之和；例如15=1+2+3+4+5.第一个三角形数T_1等于1，其后为$T_2=3$，$T_3=6$，等等，见图15所示.算术级数1，2，3，4，…，r之和是$r(r+1)/2$，它就是T_r的值.

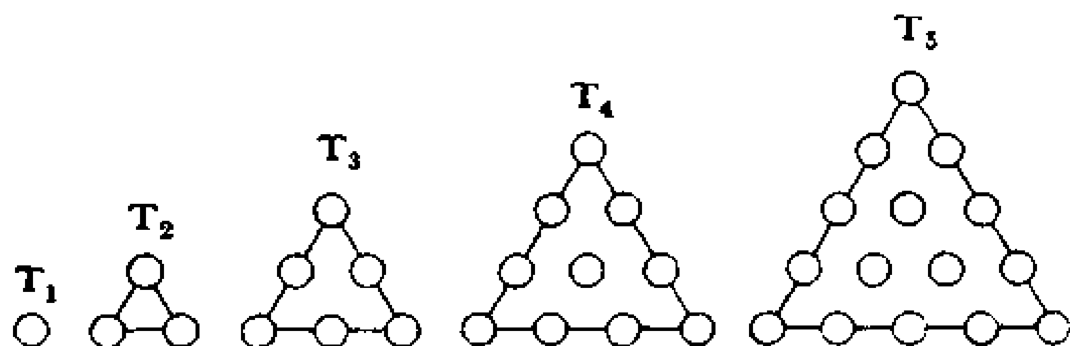
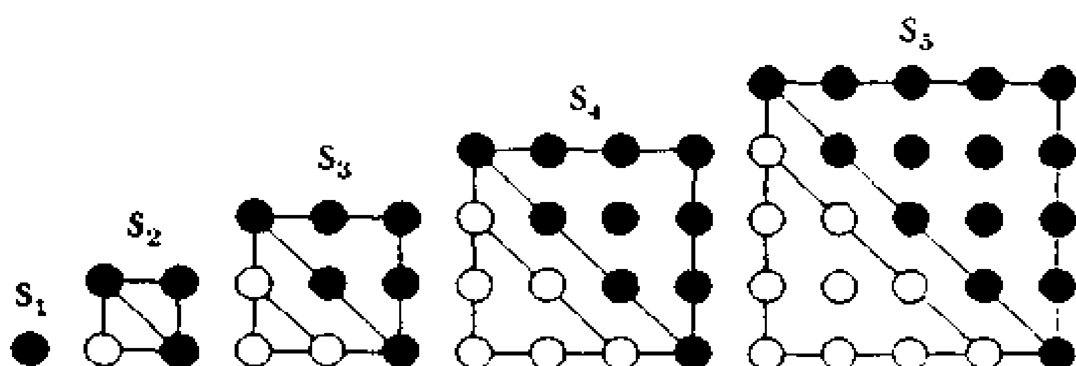


图15　三角形数

筹码或小球也可以像16那样排列成正方形阵列.当然它们可以称为"正方形数"并服从级数1，4，9，16，25，…的模式.从图中黑圈与白圈的配置状况可以看出，第一个三角形数1与第二个三角形数3合在一起就形成了第二个正方形数4；第二、三个三角形数3与6可形成第三个正方形数9；一般说来，若S_r为第r个正方形数，则有关系式$S_r=T_r+T_{r-1}$.此关系可证明如下：



[185] 图 16 正方形数

由于

$$T_r = r(r+1)/2,$$
$$T_{r-1} = (r-1)(r-1+1)/2 = (r-1)r/2,$$

相加后得

$$T_r + T_{r-1} = r(r+1+r-1)/2 = r^2,$$

结果显然等于 S_r.

再多看一些例子，我们有：

T_r	=	1	3	6	10	15	21	28	36	45…
T_{r-1}	=		1	3	6	10	15	21	28	36…
$T_r+T_{r-1}=S_r$	=	1	4	9	16	25	36	49	64	81…

* * *

毕达哥拉斯的学生们习惯于歌颂一些数的符咒、奇术，他们曾对此投入了大量的才能、地位、个性与人格. 例如“神圣的数啊，你创造了神祇与凡人，请保祐我们吧！啊，神圣的‘四’，你孕育了永恒创造的源泉，”便是他们对自然数 4 所唱的赞歌. 不过，正是从这种莫名其土地堂的“摩包君婆”[①]里产生了数论的萌

① “摩包君婆”(mumbojumbo)是西非洲黑人所崇拜的守护神；通常是一些莫名其妙的符咒. ——译者注.

芽.乌思宾斯基(Uspensky)与希斯莱特(Heaslet)在他们的著作《初等数论》中说道,"……古代的数字神秘主义即使时至今日仍在占卜星相的伪装下日益兴旺发达,这一事实真令人对人类的前途产生失望,不过,话得说回来,如果没有了它[①],人类精神也就不会产生那些出类拔萃的创造,其中也包括了数论在内."

但在毕达哥拉斯的时代,奇数仍然是"男性数",而偶数是"女性数".无疑这种称呼非常贴切,因为男人一般总是脾气暴戾,好勇斗狠,而女人则是甜蜜温顺!当时,1被视为一切数的根源,2是第一个女性数,3是第一个男性数,而和 $2+3=5$ 代表婚姻(参看第3章).即便在数的王国里,女人也在男人之前!数8掌握了爱情的奥秘,因为它把男性生殖潜力3与婚姻数5相加起来了.对此,希腊人总是要用一个单词来表示它. [186]

毕达哥拉斯及其门徒实际上是一个带有强烈个人崇拜色彩的狭隘小圈子,由于它极不重视世俗事务而逐渐失去了它原先所拥有的生命力.读者们也许很熟悉那个有名的轶事,有位商人曾请教过毕达哥拉斯,他能教点什么."我能教会你怎样去计算,"几何学家说."那我已经会了,"商人答道."你是怎样去计算的?"这位 $3^2+4^2=5^2$ 的发现人问.商人嗫嚅地说,"一,二,三,四……""住口!"圣人狂叫,"你要取的四是十,或者是一个完全三角形[②],以及我们的记号."

中国人显然创造了用简单几何模式表示数的办法.这大体上在毕达哥拉斯之前五百多年,所以远在希腊人之前他们就早已知晓了一些数的性质.他们利用一个水平短划(—)或一系列的短划来表示奇数或阳性事物,而用中间断开的两个短划(--)来表示偶数或阴性事物.有一本不迟于公元前1000年写

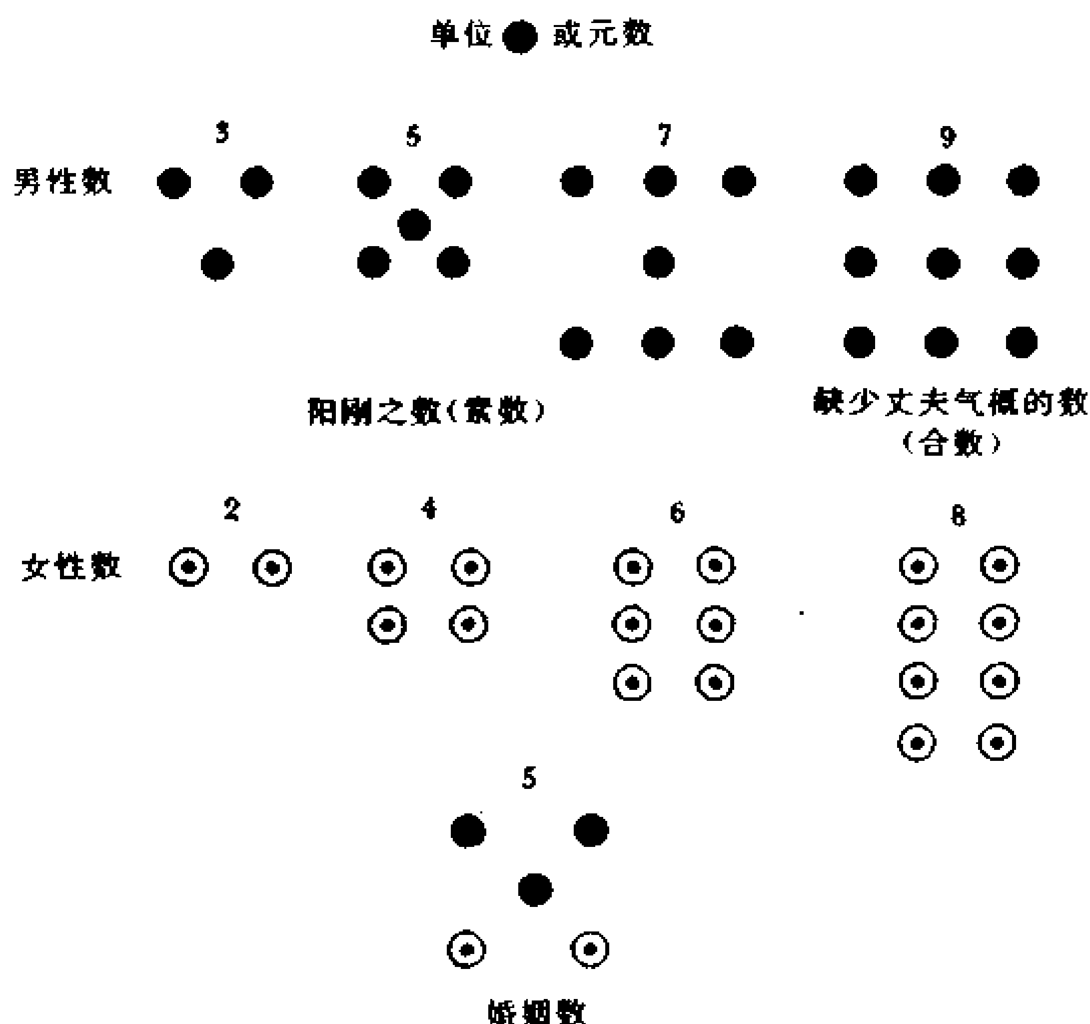
---

① 指古代数字神秘主义而不是现代迷信——占卜星相.——译者注.

② 这位圣人狂叫的"四",实际上是指第四个三角形数,即 $T_4=1+2+3+4=10$.——译者注.

成的古书上用白圈表示奇数或男性数，而用黑圈表示偶数或女性数.①

奇合数的男子气质显得不足.真正的男性应该具有严厉的不可分割性，而这种性质只是在素数身上才体现出来.因此，像9或15那样的奇合数被认为是“缺少丈夫气概的”数，但奇素数3则被认为是女性数2的佳偶，两者交配以合成婚姻数5.图17所显示的数的性别模式令人不禁想起在某些生物学教科书上所画出来的染色体排列形态图.



[187]

图17 数居然有性别

① 所指的是洛书与河图；“—”称为阳爻，“--”称为阴爻.——译者注.

序号	项(阶)				
	1	2	3	4	5
三角形数	○				
正方形数	○				
五边形数	○				
六边形数	○				
七边形数	○				
八边形数	○				

表 75 多角形数

[188]

*　　　*　　　*

既然小圆圈可排列成三角形或正方形的模式，人们自然也会想到五边形、六边形等形状. 表 75 给出了多角形数的前五个，p_n^r，从三角形数到八边形数，而表 76 则指出了每一个多角形数中所拥有的单元数，以及 n 边形多角形数的第 r 项（通项）公式.

序号	边数 n	集合数 $s=n-2$	阶数 $=r$（项）								
			1	2	3	4	5	6	7	8	r
三角形数	3	1	1	3	6	10	15	21	28	36	$\cdots r(r+1)/2$
正方形数	4	2	1	4	9	16	25	36	49	64	$\cdots r^2$
五边形数	5	3	1	5	12	22	35	51	70	92	$\cdots r(3r-1)/2$
六边形数	6	4	1	6	15	28	45	66	91	120	$\cdots r(2r-1)$
七边形数	7	5	1	7	18	34	55	81	112	148	$\cdots r(5r-3)/2$
八边形数	8	6	1	8	21	40	65	96	113	176	$\cdots r(3r-2)$
n 边形数	n	$n-2$	1	n							

$3(n-1)$　$2(3n-4)$　$5(2n-3)$

$3(5n-8)$　$7(3n-5)$　$4(7n-12)$

$(r/2)[(r-1)n-2(r-2)]$①

表 76　多角形数 p_n^r

[189]

*　　　*　　　*

有一种简单的测试法，可判明一个数是否为多角形数. 我们所要做的全部工作只是把该待决数乘以 $8(n-2)$，并在其乘积上再加 $(n-4)^2$，若结果为一平方数，则该数是一个 n 边形数；否则就不是. 例如我们想知道 45 是不是一个六边形数，可将它乘以 $8(6-2)$，得出乘积 1440，再加上 $(6-4)^2$，得 1444，而后者是 38 的平方，这就表明 45 确实是个六角形数. 要求这个多边形数

① 在用 r 与 s 表达时，此式等于 $r(rs-s+2)/2$. ——原注.

的阶，可把$(n-4)$加到平方根上，再用$(n-2)$的二倍去除其和. 以上例而言，即是 $38+(6-4)=40, 40\div 8=5$，所以阶为 5，由是可知 45 是第 5 个六角形数，如表 76 所示.

此法也可证明如下：表 76 指出，阶为 r 的 n 边形数等于$(r/2)[(r-1)n-2(r-2)]$，在将此式乘上 $8(n-2)$ 并加上$(n-4)^2$之后，结果正好是个完全平方数，其根 R 为 $2rn-4r-n+4$. 解出 r，即得

$$r=[R+(n-4)]/2(n-2),$$

这表明上述法则是正确无误的.

对给定的 n 边形数，例如从三角形数到八边形数，为了查阅方便，我们可以先算出乘数与加数以便应用于测试与求一般项. 这些数据在表 77 中已予列出.

n	乘数	加数	阶 r
3	8	1	$(R-1)/2$
4	16	0	$R/4$
5	24	1	$(R+1)/6$
6	32	4	$(R+2)/8$
7	40	9	$(R+3)/10$
8	48	16	$(R+4)/12$

表 77 n 边形数的测试

有一个极为简便的否定性测试可用来判明一个数是否三角形数. 只要把待决数的各位数码统统加起来，得出一个和数，再把和数的各位数码也相加起来，如此反复进行，直到最后只剩一个数码为止. 如果它是 2，4，5，7，8，则待决数不是三角形数；若不然，则待决数可能是，也可能不是三角形数. 现以 79 为例，此时便有 $7+9=16, 1+6=7$，故可以判明 79 不是三角形数. 再试 54，$5+4=9$，于是可知 54 不能被否定性测试排除. 进一步再使用正面测试法，由于 $54\cdot 8+1=433$，它不是一个平方数，由此判定 54 不是一个三角形数.

*　　*　　*

正如任意一个正方形数可表示为两个三角形数之和那样，[190] 一个五边形数可表示为同阶正方形数与前一阶的三角形数之和.图 18 标明了这些结果.如果用公式表示，设 r 为阶，三角形数为 T，正方形数为 S，五角形数为 P，于是有

$$S_r + T_{r-1} = P_r \quad 或 \quad (r-1)r/2 + r^2 = r(3r-1)/2.$$

一般地说，n 边形数等于其同阶的 $(n-1)$ 边形数再加上前一阶的三角形数.

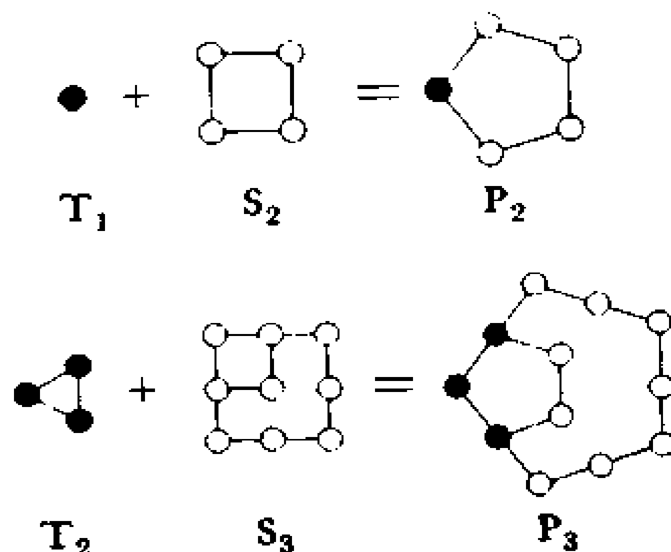


图 18　多边形数的相加

用普通代数方法可以找到各种类型的多边形数间的关系，其中有不少几何模式相当有趣.图 19 已标出了某些关系与有关的记号.

*　　*　　*

立方数 1;8;27;64;125;…与三角形数有联系:从 1 开始的连续 r 个立方数之和必定等于第 r 个三角形数的平方.例如对 $r=4$ 来说，便有

$$1^3 + 2^3 + 3^3 + 4^3 = 100,$$

图形	数的语言	图形	数的语言
	$\frac{r(r+1)}{2}+(r+1)=\frac{(r+1)(r+2)}{2}$ $p_3^r+f_1^{r+1}=p_3^{r+1}$		$4\frac{r(r+1)}{2}+(r+1)=(r+1)(2r+1)$ $4p_3^r+f_1^{r+1}=p_6^{r+1}$
	$2\frac{r(r+1)}{2}=r(r+1)$ $2p_3^r=r(r+1)$		$6\frac{r(r+1)}{2}+(r+1)=(r+1)(3r+1)$ $6p_3^r+f_1^{r+1}=p_8^{r+1}$
	$r^2+(2r+1)=(r+1)^2$ $p_4^r+f_1^{2r+1}=p_4^{r+1}$		$3\frac{r(r+1)}{2}+\frac{(r+1)(r+2)}{2}=\frac{(2r+1)(2r+2)}{2}$ $3p_3^r+p_3^{r+1}=p_3^{2r+1}$
	$8\frac{r(r+1)}{2}+1=(2r+1)^2$ $8p_3^r+1=p_4^{2r+1}$		$14\frac{2\times3}{2}+2\frac{3\times4}{2}+1=\frac{10\times11}{2}$ $14p_3^2+2p_3^3+1=p_3^{10}$
	$3\frac{r(r+1)}{2}+(r+1)=\frac{(r+1)(3r+2)}{2}$ $3p_3^r+f_1^{r+1}=p_5^{r+1}$		$2\frac{r(r+1)}{2}+(r+1)=(r+1)^2$ $2p_3^r+f_1^{r+1}=p_4^{r+1}$

图 19 多边形数

[192]

而 100 正好是第四个三角形数 10 的平方. 一般地说,

$$1^3+2^3+3^3+\cdots+r^3=[r(r+1)/2]^2=(1+2+3+\cdots+r)^2.$$

*　　　*　　　*

八个同阶三角形数再加 1,可以得出一个正方形数,当然这是对的,因为

$$8r(r+1)/2+1=4r^2+4r+1=(2r+1)^2.$$

这个有趣的关系式为一种方法奠定了基础,用此方法可以找出兼有三角形数与正方形数两重身份的数. 若我们能找到一个正方形数 X^2,使它在乘 8 再加 1 后,结果依然是正方形数,则 X^2 也必然是三角形数. 当然这种办法将要求人们去解 $8X^2+1=Y^2$,而这是一个佩尔方程,我们将在第 22 章中加以讨论. 在下面的附表 78 中给出了它的前七组解,X^2 的值既是正方形数,又为三角形数.

[191]

佩尔方程的解 $8X^2+1=Y^2$		三角形数 $=X^2$	三角形的边长 $=n$	正方形的边长 $=X$
$8\cdot1^2+1=$	3^2	1	1	1
$8\cdot6^2+1=$	17^2	36	8	6
$8\cdot35^2+1=$	99^2	1225	49	35
$8\cdot204^2+1=$	577^2	41616	288	204
$8\cdot1189^2+1=$	3363^2	1413721	1681	1189
$8\cdot6930^2+1=$	19601^2	48024900	9800	6930
$8\cdot40391^2+1=$	114243^2	1631432881	57121	40391

表 78　兼有正方形数与三角形数双重身份的数

这个佩尔方程中 X 的一般解将在本章晚些时候给出.

*　　　*　　　*

多边形数只是所谓"拟形数"中的一种而已. 拟形数中的第一族或"线性族"实际上不过是从 1 开始的算术级数. 如果 d 是公差,则 $1,1+d,1+2d,\cdots,1+(r-1)d$ 便是该线性族从第 1 项到第 r 项的相继各项. 如果令 $d=1$ 与 $d=2$,则可得到这一族

的两个集合 1,2,3,4,5,…,$(r-1)$;1,3,5,7,9,…,$(2r-1)$.显然在族中的第 s 个集合中 $d=s$,而级数变成 $1,1+s,1+2s,1+3s,\cdots,1+(r-1)s$.我们可以使用记号 $f^r_{1,s}$来表示拟形数的线性族,这里 1 代表拟形数中族的序号(也叫维数)m,而 s 代表集合号码,r 则为集中的阶.例如 $f^5_{1,2}=9$,$f^4_{1,1}=4$.

如果我们把上述级数的各项之和作为新级数中的项,以形成自 1 开始的新级数,于是我们得到 $1,3,6,10,15,\cdots,r(r+1)/2$;$1,4,9,16,25,\cdots,r^2$;第 s 个级数将是 $1,2+s,3+3s,4+6s,\cdots,r(rs-s+2)/2$.

这些级数不再是算术级数.值得注意的是,它们是表中的多边形数,而 $s=n-2$.

这些“和-级数”的各项称为“平面拟形数”;此种数目的维数 $m=2$.因而一切平面拟形数都可用记号 $f^r_{2,s}$来表示,与之对应的通常记号则为p^r_{n-2}.从而有$f^4_{2,2}=p^4_4=16$,$f^7_{2,1}=p^7_3=28$,$f^5_{2,s}=p^5_{n-2}=10s+5=10n-15$.一般说来,一个多边形数等于首项为 1,公差 d 为 $n-2$ 的算术级数之和.例如在六边形数中 $n=6$,公差是 $6-2=4$,而六边形数便是此种算术级数之和.毕达哥拉斯学派的人把算术级数的项称为“磬折形”①. [193]

类似地可以通过不断求和办法得出“立体”的,也就是三维拟形数,此时 $m=3$.这种数目有时也称为“棱锥数”或“锥形数”.它们可记为 $f^r_{3,s}$或 P^r_{n-2},其意思是第 s 个棱锥的第 r 个数.表 79 给出了锥形数,大家不妨拿它来同表 76 的多边形数对比一下.查一下表 79,即可知道 $f^6_{3,5}=P^6_7=196$.

“锥形数”这一名称也许蕴含着某种意思,即该数等于某个锥形数的、形状对称的物体,例如像小球可以堆积成均匀对称的

---

① 磬折形是在平行四边形的角上截去一较小而与原形相似的平行四边形后所得之图形.毕氏学派持有“凡物皆数”的强烈信念,他们认为几何图形也可以用数来解释.当然图形并不限于平行四边形,故也有译作“心射形”的.——译者注.

底的种类	底的边数 $=n$	集合数 $s=n-2$	阶 r 1	2	3	4	5	6	7	8	r
三角形	3	1	1	4	10	20	35	56	84	120	$\cdots r(r+1)(r+2)/6$
四边形	4	2	1	5	14	30	55	91	140	204	$\cdots r(r+1)(2r+1)/6$
五边形	5	3	1	6	18	40	75	126	196	288	$\cdots r^2(r+1)/2$
六边形	6	4	1	7	22	50	95	161	252	372	$\cdots r(r+1)(4r-1)/6$
七边形	7	5	1	8	26	60	115	196	308	456	$\cdots r(r+1)(5r-2)/6$
八边形	8	6	1	9	30	70	135	231	364	540	$\cdots r(r+1)(2r-1)/2$
…											
n 边形	n	$n-2$	1	$n+1$	$2(2n-1)$	$10(n-1)$	$5(4n-5)$	$7(5n-7)$	$28(2n-3)$	$12(7n-11)$	$[r(r+1)/6][(r-1)n-(2r-5)]$①

表 79 锥形数 P_n^r

棱锥，但这仅仅是对正三棱锥（底面为正三角形）与正四棱锥（底面是正方形）才有可能. 在其他情况下，由多边形数给出的各层小球并不能均匀地分布于三维空间. 例如，对每边只有 2 个小球（总数为 6 个小球）的六角形底面来说，如果要堆成二级棱锥，则中间就有足够的地位可安置一个外加的小球，而它是第 2 个六角形数所没有计算进去的；对第四阶来说，更须在底上额外再追加 9 个更多的小球，而这些都是在该阶六角形数 28 以外的. 看一下表 75 即可理解.

[194]

但是，在底为正三角形或正方形时，小球可以堆垒成均匀的

① 在用 r 与 s 表达时，此式等于 $r(r+1)(rs-s+3)/6$. ——原注.

棱锥，而球的总数是一个锥形数. 以正方形为底而每边有 5 个小球的棱锥将使用 55 个小球，即 $f_{2,2}^5=P_4^5=1+4+9+16+25=55$.

锥形数 P_n^r 可通过下列公式，从相应的多边形数 p_n^r 中极为方便地算出来：

$$P_n^r=(r+1)(2p_n^r+r)/6.$$

读者们也许想用表 76 与表 79 中的多边形数与锥形数来验证上述关系式. 例如：

$$p_6^7=91, P_6^7=(7+1)(2\cdot 91+7)/6=252.$$

正如 n 边形数是同阶 $(n-1)$ 边形数与前一阶的三角形数之和那样，任一 n 角锥形数是同阶 $(n-1)$ 角锥形数与前一阶的三角锥(四面体)形数之和. 例如，第 7 阶六角锥形数 P_6^7 是 252，它等于 7 阶五角锥形数 196 与 6 阶三角锥形数 56 之和. 一般地，对锥形数有

$$P_n^r=P_{n-1}^r+P_3^{r-1};$$

而对多边形数有

$$p_n^r=p_{n-1}^r+p_3^{r-1}.$$

多边形数可以用平面上的多边形来说明，锥形数则可通过棱锥予以图解. 尽管我们无法用四维或更高维的几何模式来对以锥形数的和为项的新级数进行直观说明，但至少可以从解析角度来对它们进行研究. 由锥形数的求到 r 阶的和作为级数的项，用此办法可以得到四维拟形数 $f_{4,s}^r$，它们已在表 80 中列出.

最后，我们把此种步骤加以一般化，即可得出 m 维拟形数：

$$f_{m,s}^r=(rs+m-s)(r+m-2)!/m!(r-1)!.$$

有了这个简单公式，不管什么样的拟形数，只要已知维数 m，集合数 s，与阶数 r，就都能求出来.

生成多边形	集合数 $=s$	阶 $=r$								
		1	2	3	4	5	6	7	8	r
三角形	1	1	5	15	35	70	126	210	330	$\cdots r(r+1)(r+2)(r+3)/4!$
正方形	2	1	6	20	50	105	196	336	540	$\cdots r(r+1)^2(r+2)/12$
五边形	3	1	7	25	65	140	266	462	750	$\cdots r(r+1)(r+2)(3r+1)/4!$
六边形	4	1	8	30	80	175	336	588	960	$\cdots r^2(r+1)(r+2)/6$
七边形	5	1	9	35	95	210	406	714	1170	$\cdots r(r+1)(r+2)(5r-1)/4!$
八边形	6	1	10	40	110	245	476	840	1380	$\cdots r(r+1)(r+2)(6r-2)/4!$
$(s+2)$边形	s	1	$(s+4)$	$5(s+2)$	$5(3s+4)$	$35(s+1)$	$14(5s+4)$	$42(3s+2)$	$30(7s+4)$	$r(r+1)(r+2)(rs-s+4)/4!$

[195]

表 80　四维拟形数 $f_{4,s}^r$

在 $s=1$ 时，即对应于第一集合，我们有：

$$
\begin{aligned}
f_{m,1}^r &= (r+m-1)(r+m-2)!/m!(r-1)! \\
&= (r+m-1)!/m!(r-1)! \\
&= r(r+1)(r+2)\cdots(r+m-1)/m! \\
&= (m+1)(m+2)(m+3)\cdots(m+r-1)/(r-1)!.
\end{aligned}
$$

读者们也许会认出它就是二项式系数，或者组合数 C_{r+m-1}^m（或 C_{r+m-1}^{r-1}，由组合基本性质，这是显然的）.

像表 76，表 79，表 80 是对二维，三维，四维拟形数造的那样，m 维拟形数的一系列表格也可以造出来. 如果把这些表格统统集拢在一起，它们将能形成一张拟形数的三维表格.

*　　　　*　　　　*

有关拟形数的趣题不少，一般是要求它们进一步满足一些

附加条件.

1. 求一正方形数,它能表示以正方形为底面的棱锥中的球数,换言之,P_4^r 必须是个平方数. 这种数只有一个. 在 $r=24$ 时,将有 $1^2+2^2+3^2+\cdots+24^2=4900=70^2$.

[196]

2. 要求在三角锥(四面体)中的球数 P_3^r 是平方数,这样的解只有两个,即 $2^2=1+3$ 与

$$140^2 = 1 + 3 + 6 + 10 + \cdots + 1176.$$

3. 任何一个三角形数不可能是立方数,四次幂或五次幂.

4. 锥形数不可能同时又是立方数或五次幂,除了上述例子以外,它们甚至不是平方数.

5. 如表 78 所示,三角形数可以是平方数. 它们可从级数 0,1,6,35,204,…,u_n 中找到,这里,$u_n=6u_{n-1}-u_{n-2}$. 即每一项是前一项的六倍,再减去更前面一项. 此种数目的平方兼有两重身份,既是平方数,又是三角形数.

很像是第 14 章中讲过的、求毕氏三角形连续数边的那个公式,求上述两重身份的三角形数时,也可不必用上面的级数,而改用公式:

$$\left\{\left[(1+\sqrt{2})^{2x}-(1-\sqrt{2})^{2x}\right]/4\sqrt{2}\right\}^2.$$

当 x 相继取值 1,2,3,…时,我们即能像上面一样地得出 1,6,35,…,但它当然要比前一种办法麻烦得多.

6. 除 1 之外,三角形数 6 是唯一的例子:其平方也是一个三角形数,下一个例子将有 660 位以上数码. 这个条件要求表 78 中的 X 是一个三角形数.①

7. 三角形数 55,66,666 是组成数码在 30 位以内的唯一由

① 原文如此,说法较含糊,但与第 5 题并不矛盾. 因为 35 的平方虽同时为三角形数与平方数,然而 35 本身不是三角形数,但 6 却不一样. ——译者注.

相同数码组成的几个实例.

8. 试求一些三角形数,它们的和与差也是三角形数. 表 81 中给出了一些解答.

第一个 $F=$ $x(x+1)/2$	第二个 $S=$ $y(y+1)/2$	三角形之边长 x	y	和= $F+S=$ $Z(Z+1)/2$	差= $F-S=$ $V(V+1)/2$	三角形的边长 Z	V
21	15	6	5	36	6	8	3
171	105	18	14	276	66	23	11
990	780	44	39	1770	210	59	20
3741	2145	86	65	5886	1596	108	56
2185095	1747515	2090	1869	3932610	437580	2804	935

[197] **表 81 三角形数对子,其和与差也是三角形数**

9. 求一个 m 边形数,它同时又是 n 边形数. 我们已讲过兼为三角形数与正方形数的数. 三角形数而同时又是五边形数的例子有 1,210,40755.

10. 仅当 $2r+1=3u$,而

$$u = 1,3,17,\cdots,u_n = 6u_{n-1} - u_{n-2}$$

时,三个连续三角形数的乘积 $p_3^{r-1}\cdot p_3^r\cdot p_3^{r+1}$ 是一个平方数. 例如 $u=3$ 时,$r=4$,这时第三,第四,第五个三角形数 6,10,15 的乘积等于平方数 900. 当 $u=17$ 时,$r=25$,而

$$p_3^{24}\cdot p_3^{25}\cdot p_3^{26} = 300\cdot 325\cdot 351 = 34222500 = 5850^2.$$

*　　　*　　　*

尽管涉及拟形数与多边形数的许多定理与问题大都只属初等性质,但在此领域中也有一些初等手段远远不能解决的问题. 例如,任一正整数要么本身就是一个三角形数,要么是两个三角形数之和,要么最多是三个三角形数之和;任一正整数是最多四个平方数之和;一般说来,任一正整数是最多 m 个 m 边形数之和. 虽然立方数与四次幂不属于上述讨论范畴,但也可以顺便在

此指出：任一正整数是最多 9 个立方数或最多 19 个四次幂之和.

表 76 中有关五边形数的那一行显示出它们遵循数列：1；5；12；22；35；…，一般项是 $r(3r-1)/2$. 若将此式修改为 $r(3r\pm1)/2$，则由此通项公式概括而得的数 1；2；5；7；12；15；22；26；35；40；…称为"广义"五边形数. 这些广义五边形数在欧拉发明的一个著名公式中着实露了一手. 一个正整数 N 的所有除数之和有时可记为 $S(N)$（参看第 3 章）. 欧拉公式如下：

$$S(N)-S(N-1)-S(N-2)+S(N-5)+S(N-7)$$
$$-S(N-12)-S(N-15)+S(N-22)+S(n-26)$$
$$-S(N-35)-S(N-40)+\cdots=0.$$

在此公式中，从第一项之后，加号与减号双双交替出现，并且用上了广义五边形数. 但需对此公式略作说明. 只要括弧里头的数是非负数，计算就可以继续进行下去. 另外要对 $S(0)$ 作出解释，否则它是无意义的. 我们规定 $S(0)$ 就等于 N. 例如，取 $N=15$，于是就有： [198]

$$S(15)-S(14)-S(13)+S(10)+S(8)-S(3)-S(0)=0.$$

15 的除数为 1；3；5；15，其和是 24. 14 的除数为 1；2；7；14，其和正巧也是 24. 类似地做下去，可以算出 $S(13)=14$；$S(10)=18$；$S(8)=15$；$S(3)=4$；$S(0)=15$，于是有 $24-24-14+18+15-4-15=0$.

数 15 碰巧是个五边形数；让我们另外换一个不是五边形数的 27 来再试一试，这时，$S(0)$ 不出现了：

$$\begin{aligned} S(27)-S(26)-S(25)+S(22)+S(20)-S(15) \\ -S(12)+S(5)+S(1) &= 40-42-31+36+42 \\ &\quad -24-28+6+1 \\ &= 0. \end{aligned}$$

一般总是认为，除数之和与五边形数是南辕北辙，毫无关系可言的. 这个公式的出现真是令人不可思议.

参考文献

Barlow, P. *Theory of Numbers*. London: J. Johnson & Co., 1811.

Danzig, T. *Number: The Language of Science*. New York: Macmillan Co., 1954.

Dickson, L. E. *History of the Theory of Numbers*. 3 vols. New York: Chelsea Publishing Co., 1950.

Hall, H. S., and Knight, S. R. *Higher Algebra*. New York: Macmillan Co., 1932.

Hogben, L. *Mathematics for the Million*. New York: W. W. Norton & Co., 1951.

Lucas, E. *Récréations Mathématiques*. Paris: Gauthier-Villars et Cie., 1882.

Uspensky, J. V., and Heaslet, M. A. *Elementary Number Theory*. New York: McGraw-Hill Book Co., 1939.

[199]

第19章 黄金定理

"黄金定理","高等算术的明珠"——这些是卡尔·弗利特列希·高斯对于平方互反律的热情洋溢的颂辞.当然这些都是当之无愧的,它的的确确是数论定理中的一颗珍珠.

平方互反律,也叫"勒让德二次互反律",首先由勒让德(A. M. Legendre)明确宣布,尽管著名的欧拉在多年以前已对这种素数所具的性质作过介绍.但是勒让德本人无力对此提供一个无瑕可击的证明,这种事情只好留给了伟大的高斯去做.高斯真是名不虚传,他成功地获得了该定律的七个不同证明,而其中的第一个证法是他年仅19岁时取得的.高斯的成就无疑大大地激励了后人,其他研究家们又不断发现新证法,以至目前二次互反律的证法不少于50个.

根本不知道欧拉与勒让德曾作过研究的高斯纯粹通过观察而发现了这一定理.他用了整整一年光阴来证明它.他说,"它全年都在折磨着我,尽管我竭尽全力,它总是巧妙地躲过追捕.可是,最后我还是得到了它的证明,这已写在《算术专题研究》的第四部分中"——这本书是高斯的巨著.

要想理解定理的文字叙述也不太容易,在此之前,我们先得知道一点有关二次剩余——平方的余数——的知识以及一些专用记号.

如果我对你说:"求一个平方数,当用11去除它时,会得出余数2,"你当然充分理解我的意思.于是,便从垂手可及的地方

拿起纸和笔来，迅速写下一些平方数，再通过心算，用 11 去除它们，你心中自会有所感觉，只要略试几次，便可找到答案. 或许在你的书包里有一张平方数表，可以一下子就试除前 20 个或诸如此类的平方数，结果却十分惊讶：竟然没有一个平方数能留下余数2来！一般人的想法原也未可厚非，因为人们会“直觉”地感到，用 11 去除时，从 0 到 10 的余数都可能出现. 然而，当你仔细察看一下时将会发现，只能找到 0，1，3，4，5，9 等余数，而从来没有 2，6，7，8，10 这些余数.

[200]

对一个给定的模数来说，并不是所有的数都能作为平方余数的，用 11 做模数就可以用来说明这一事实. 任一正整数都必然是下列形式之一：$11x$，$11x\pm1$，$11x\pm2$，$11x\pm3$，$11x\pm4$，$11x\pm5$. 因而其平方必为下列形式之一：$121x^2$，$(121x^2\pm22x+1)$，$(121x^2\pm44x+4)$，$(121x^2\pm66x+9)$，$(121x^2\pm88x+16)$，$(121x^2\pm110x+25)$. 这些表达式对模 11 来说，同余于 0，1，4，9，5，3. 因而，只有这些整数才是模 11 的**平方剩余**，而 2，6，7，8，10 是一个平方数被 11 去除时从来不会出现的余数，它们叫做模 11 的**平方非剩余**.

表 82 给出了从 3 到 29 的一切奇素数的平方剩余与非剩余. 应当指出，对任一素数来说，平方剩余与非剩余的个数总是相等的.

如果存在一平方数 x^2，使 $x^2\equiv r \pmod m$，则整数 r 称为 m 的平方剩余，但当 m 为合数时，与它不互质的平方剩余通常是要排除掉的，因而即使 $9^2\equiv6 \bmod 15$ 成立，6 仍然不认为是 15的平方剩余. 为了简单起见，以下讨论将只限于奇素数模.

在解二次同余式(例如 $2x^2-5x\equiv7 \bmod 23$)或说明二次同余式无解时不可避免地要用到平方剩余的知识. 平方剩余也可以巧妙地应用于数的因子分解，本书第 21 章将加以阐述. 其实，在讲梅桑数与原根时已经提到过.

素数	剩余	非剩余
3	1	2
5	1,4	2,3
7	1,2,4	3,5,6
11	1,3,4,5,9	2,6,7,8,10
13	1,3,4,9,10,12	2,5,6,7,8,11
17	1,2,4,8,9,13,15,16	3,5,6,7,10,11,12,14
19	1,4,5,6,7,9,11,16,17	2,3,8,10,12,13,14,15,18
23	1,2,3,4,6,8,9,12,13,16,18	5,7,10,11,14,15,17,19,20,21,22
29	1,4,5,6,7,9,13,16,20,22,23,24,25,28	2,3,8,10,11,12,14,15,17,18,19,21,26,27

表 82 平方剩余与非剩余

有一个简单方法可以确定数 r 是不是素数 p 的平方剩余.若 $r^{(p-1)/2}\equiv+1 \bmod p$,则 r 是平方剩余;若 $r^{(p-1)/2}\equiv-1$,则它是平方非剩余.同余数右边的数要么是+1,要么是-1,决不能是其他整数,因而 r 是不是 p 的平方剩余,只要看一看就模 p 而言,$r^{(p-1)/2}$究竟是同余于+1 还是-1.勒让德符号$(r|p)$(其值只能取+1 或-1)是一个极其简洁的记号,它表明了 r 对于素数 p 的"平方性态".在 $r=2$,$p=11$ 时,$2^{(11-1)/2}=2^5\equiv-1 \bmod 11$,所以 2 是 11 的平方非剩余,即$(2|11)=-1$;但对 $r=3$ 来说,$3^5=243\equiv+1 \bmod 11$,因此 3 是一个平方剩余,于是$(3|11)=+1$.

[201] 容易证明这一测试的正确性,因若r是p的一个平方剩余,则必意味着存在一个平方数 x^2,使关系式 $r\equiv x^2 \bmod p$ 成立,将此同余式的两边都抬升到$(p-1)/2$ 次幂,我们即有:

$$r^{(p-1)/2}\equiv(x^2)^{(p-1)/2}\equiv x^{p-1},$$

由费马定理,x^{p-1}必定是关于模 p 同余于 1 的.

这一测试虽然是结论性的,但当模与剩余很大时,计算量相当大,因而人们还需要更切合实用的办法.高斯的黄金定律,也就是二次互反律便是这样一种测试法;它使人们有可能确定一个奇素数 p 是否另一个奇素数 q 的平方剩余,所采用的办法竟是反其道而行之:先确定 q 是不是 p 的平方剩余.定理断言$(p|q)=(q|p)$,除非 p,q 都是 $4x-1$ 形式的素数,在那种情况下将有$(p|q)=-(q|p)$.例如,要想知道 3 对素数 13 的平方性态,由于 3 与 13 并非都是 $4x-1$ 形式的素数,故有$(3|13)=(13|3)$.由于记号$(13|3)$实际上是同余式 $x^2\equiv13 \bmod 3$ 的一种浓缩写法,而后者在去掉 3 的倍数后,可简化为 $x^2\equiv1 \bmod 3$,因此,$(13|3)$与$(1|3)$是一样的.但是 1 是 13 的平方剩余,从而$(13|3)=+1$,于是$(3|13)=+1$,因此 3 是 13 的平方剩余,而实际

上确有 $4^2 \equiv 3 \bmod 13$.

再试一次，由于29与1193都是 $4x+1$ 形式，于是得出 $(29|1193)=(1193|29)=(4|29)$（此步是从1193中减去了29的倍数）. 显然 $(4|29)=+1$，因为4本身就是一个用29去除它时余数为4的平方数. 于是 $(29|1193)=+1$，但是真要找出一个平方数，使得用1193去除它时留下余数29却要困难得多，让我们留到以后去说. 读者们自己能找出它吗？†

两个剩余之积或两个非剩余之积是一个剩余（当然是对同样的模来说）；一个剩余与一个非剩余之积是一个非剩余. 例如，若 $(r|p)=+1$，$(s|p)=-1$，$(t|p)=-1$，则 $(rs|p)=-1$，$(st|p)=+1$ 等等. 这是因为：若 $(r|p)=+1$，$(s|p)=-1$，则有 $r^{(p-1)/2} \equiv 1$，$s^{(p-1)/2} \equiv -1 \bmod p$，由同余式的性质，当然就有 $(rs)^{(p-1)/2} \equiv -1 \bmod p$，等等.

我们可把它应用于二次互反律的另一例子. 正整数19与31都是 $4x-1$ 形式的素数，于是 $(19|31)=-(31|19)=-(12|19)$. 但 $-(12|19)$ 可记为

$$-(3|19)(4|19)=-(3|19)\cdot(+1),$$

[203]

因4是一个平方数，故可作这样的简化. 再继续做下去，$-(3|19)=--(19|3)=+(1|3)=+1$，因此19是31的平方剩余. 此时，一眼即可看出平方数81就是解，但当然这只是碰巧. 上述内容仅不过是一种测试，而不是求解的办法.

* * *

在特定情况下求 $(p|q)$ 值当然也不错，但比它更有趣、更具有普遍意义的是找出一大类素数而能使一个给定整数恒为平方剩余. 例如，对 $4x+1$ 形式的任一素数，-1 恒为平方剩余；对 $8x+1$ 或 $8x-1$ 形式的任一素数，2恒为平方剩余. 这两条规则与二次互反律可以巧妙地表达如下：

数学表达式	意　义
(a) $(-1\mid p)=(-1)^{(p-1)/2}$	-1 是形式为 $4x+1$ 的一切素数 p 的平方剩余，再无其他.
(b) $(2\mid p)=(-1)^{(p^2-1)/8}$	素数 2 是形为 $8x\pm1$ 的一切素数 p 的平方剩余，再无其他.
(c) $(p\mid q)(q\mid p)=(-1)^{(p-1)(q-1)/4}$	素数 p 对素数 q 的平方性态与 q 对 p 的平方性态相同或相反，这要看 p,q 中至少有一个，或全然没有 $4x+1$ 形式的素数而定.

设我们要找出 10 是平方剩余的一类素数所应有的形式. 由于 $(10\mid p)=(2\mid p)(5\mid p)$，由此可见若 $(2\mid p)$ 与 $(5\mid p)$ 都是 $+1$ 或都是 -1，则 10 是 p 的平方剩余. 先假定两者都为 $+1$. 由上述的(b)式可知，仅当 $p=8x\pm1$ 时，才能使 $(2\mid p)=+1$；由于 5 是 $4x+1$ 形的素数，于是 $(5\mid p)=(p\mid 5)$. 但 5 的平方剩余是 1 与 -1，因此 p 的形式必为 $5y\pm1$. 要想同时兼有 $8x\pm1$ 与 $5y\pm1$，可见 p 必为 $40x\pm1$ 或 $40x\pm9$ 中之一，从而可知 10 是这四类形式的素数的平方剩余，例如 41，79，89，31.

再来看 $(2\mid p)=-1$ 与 $(5\mid p)=-1$ 的情况，若 p 为 $8x\pm3$ [204] 的形式，则第一式肯定成立，由于 $(5\mid p)=(p\mid 5)=-1$，第二式对 $p=5y\pm2$ 是成立的，这是由于 5 的平方非剩余是 2，3，也就是 ±2 之故. 要使 p 同时兼有 $8x\pm3$ 与 $5y\pm2$，则 p 必须取 $40x\pm3$ 或 $40x\pm13$ 的形式.

综上可知，对下列八种形式：$40x\pm1$，$40x\pm3$，$40x\pm9$，$40x\pm13$ 的一切素数，10 都是平方剩余.

第 11 章中，寻找 10^2-1（2 是一个素数）形式的数的因子时是利用了这个事实的. 对上述八种形式的 p，我们已有关系式

$$10^{(p-1)/2} \equiv 1 \mod p,$$

因而如果$(p-1)/2$也是一个素数z时，则10^z-1将能被p整除. 而这仅仅对$p=40x-1, 40x+3, 40x-13$是成立的，其他情况下$(p-1)/2$都是合数，由此而得：

$$10^{20x-1} \equiv 1 \mod 40x-1,$$
$$10^{20x+1} \equiv 1 \mod 40x+3,$$
$$10^{20x-7} \equiv 1 \mod 40x-13.$$

在$x=2$时，有$20x+1=41, 40x+3=83$，两者都是素数，由此可知$10^{41} \equiv 1 \mod 83$.

* * *

二次互反律的证明对我们来说是太深奥了一点，但它实在是巧妙透顶，因此导致最终证明的步骤至少还是应当说一说. 至于定理的完全证明，请读者自己去参看一本现代的数论教科书.

1. 若整数m不能被素数p整除，取m的倍数$1m, 2m, 3m, \cdots, [(p-1)/2]m$，如果在这些数的关于模$p$的最小正剩余数中，超过$\frac{p}{2}$的个数是偶数，则$m$是$p$的平方剩余；若超过$\frac{p}{2}$的个数为奇数，则$m$是$p$的平方非剩余. 这一事实，通常称为高斯引理，若$r$为这种正剩余的个数，则我们可以把上述引理简洁地记为$(m|p)=(-1)^r$.

例如，取$p=13, m=3$，则$(p-1)/2=6$，现在写出m的六个倍数，

$$3, 6, 9, 12, 15, 18.$$

这些倍数对模13的最小正剩余为：

$$3, 6, 9, 12, 2, 5,$$ [205]

其中有两个数9与12超过了$\frac{p}{2}$. 因为2是一个偶数，所以整数

$m=3$ 是 13 的一个平方剩余. 如果有五个剩余数超过 $\frac{p}{2}$ 的话,则因 5 是个奇数,于是 m 就将是一个平方非剩余了.

2. 由上述性质可知,若 p,q 是两个素数,r,s 分别为 $1q,2q,3q,\cdots,[(p-1)/2]q$ 以及 $1p,2p,3p,\cdots,[(q-1)/2]p$ 对模 p 与模 q 的最小正剩余数中超过 $\frac{p}{2}$ 与 $\frac{q}{2}$ 的数的个数,则必有

$$(p|q)(q|p)=(-1)^r(-1)^s=(-1)^{r+s}.$$

3. 仅当 p,q 都是 $4x-1$ 形式的素数时,和数 $r+s$ 才能为奇数,只有在此种情况下 $(p|q)(q|p)=-1$. 由此即可推出前面说过的二次互反律. 第三步的证明是连高斯也感到很头痛的.

* * *

原根的一项有趣性质也进入了平方剩余领域. 任何原根的偶数次幂是素数 p 的平方剩余,而奇数次幂是平方非剩余. 例如,2 是 13 的原根,于是 $2^2,2^4,2^6,2^8,2^{10},2^{12}$ 分别同余于 4,3,12,9,10,1,它们都是 13 的平方剩余. 另一方面,$2^1,2^3,2^5,2^7,2^9,2^{11}$ 则分别同余于 2,8,6,11,5,7,它们都是 13 的平方非剩余.

* * *

当一数已被确定为某个给定素数的平方剩余之后,真正要具体找出剩余为该已知数的平方数是颇为困难的. 下面的一些规则可适用于若干特例.

1. $x^2\equiv-1 \bmod p=4n+1$ 的解是

$$x\equiv\pm[(p-1)/2]!.$$

2. $x^2\equiv a \bmod p=4n+3$ 的解是

$$x\equiv\pm a^{n+1}.$$

3. $x^2\equiv a \bmod p=8n+5$ 的解是

$$x \equiv \pm [(4a)^{n+1}]/2.$$ [206]

4. $x^2 \equiv a \mod p = 8n+1$:

除非 $a=\pm 2$ 否则无解.

当 $a=\pm 2$ 时,$x^2 \equiv \pm 2 \mod p=8n+1$ 的解是

$$x \equiv g^n \pm g^{7n} \mod p,$$

这里,g 是 p 的一个原根.

*　　　*　　　*

解二次同余式的一个巧妙而实用的办法是利用排除法.求解二次同余式 $x^2 \equiv b \mod p$ 当然等价于解方程:$x^2=b+py$,即要找出 p 的某个倍数 py,使它加到 b 之后得出一个平方数.即使对相当大的 b,p 值,要进行试验的 y 值也可以作出限制,以便做到只要通过少量试验即可求出解来.如果上述方程联系到一个较小的模数 E,则并非所有的 y 值都能使 $b+py$(也就是 x^2)成为 E 的平方剩余(由于 x^2 是个平方数,这意味着 $b+py$ 必须为平方剩余).于是 y 的这些值即可排除.

设我们要解二次同余式 $x^2 \equiv 33 \mod 97$或与之等价的方程 $33+97y=x^2$,当然第一步先要用二次互反律进行测试,得到正面结果后再进行.第二步,取任意模数 5,于是方程的左边成为 $3+2y$.对模 5 来说,y 可以是 0,1,2,3,4;而 $3+2y$ 将会同余于 3,0,2,4,1.但要使 $b+py$ 是个平方数,它必须同余于 5 的一个平方剩余,即 0,1 或 4;因此,使 $3+2y$ 等于 2 或 3 的那些 y 值就必须排除.从而 y 只能按模 5 同余于 1,3,4.所以具有 $5z$ 或 $5z+2$ 形式的那些 y 值就不必试了.类似地,对所取的很小模数 7 来说,y 只能取 $7z+1$,$7z+3$,$7z+4$ 或 $7z+5$ 等形式;而 $7z$,$7z+2$,$7z+6$ 等必须排除.还可以用类似办法取 8,9,11,13 等数(素数或素数之幂),并从中排除掉一些不可能的形式,但对如此小的模数 97 来说,用 5 与 7 作为排除元已经足以限制 y 了.

另外，超过$\frac{p}{4}$的 y 值根本用不着试，因为如果方程的解是 x，则 $p-x$ 也必定是解（x^2 按模 p 同余于$[p-x]^2$，因而 x 或 $p-x$ 小于$\frac{p}{2}$，于是 x^2 或$[p-x]^2$ 就小于$\frac{p^2}{4}$）. 因而 py 必小于 $p^2/4$，即y小于$p/4$. 于是，我们可以列出一张连续正整数表格，[207] 从 1 开始，不超过 24，并删掉其中 $5z$ 或 $5z+2$ 形式的数，留下 1，6，11，16，21，3，8，13，18，23，4，9，14，19，24. 从这些数值中继续删掉 $7z$，$7z+2$ 与 $7z+6$ 形式者，最后留下 1，3，4，8，11，18，19，24. 略为试一下，其中的第二个数就给出了方程的一个解答，因为 $33+97\cdot 3=324=18^2$. 第二个解是 $97-18=79$.

由较小模数产生的排除元表格已经造了出来，通过这种表格，人们已能很快解出较大模数的二次同余式. 对上例来说，排除法看来似乎并不是很有效的，但如果要去解本章以前曾提到过的二次同余式 $x^2\equiv 29 \bmod 1193$，若利用 5，7，8，9，11，13 作为排除元，则待试的 y 值即可从 298 个减少到 4 个. 为了进一步削减工作量，人们可以购入或自制一套模板，这种套上，在指定间距处就不同模数镂刻了一些洞孔. 把模板叠合起来时，有的洞孔会重合，这就是几种形式同时可以成立的数字. 利用数字计算机，数以百万计的数可以迅速地得到检验而无需人的参预.

* * *

对一个给定的模数，人们常常需要知道它的一些较小的平方剩余数. 在把模分解成因子或者确定模是素数时，这种平方剩余能起相当作用. 本书第 21 章将讨论这种分解法，这里想讲一讲怎样才能求出较小平方剩余的办法，这种方法相当巧妙并且也容易理解. 设想我们要求出数 $N=135287$ 的五个平方剩余，其中的每一个都小于 250. 首先可找到一个较 N 略大一些的最小平方数 n^2，对本例来说是 $368^2=135424$. 于是有 $n^2-N=137$，由于 368^2 除以 135287 留下了这个剩余，故知 137 是 135287 的一个平方剩余. 用类似办法可求出 369^2，370^2 等数的平方剩余

数.实际上,不需要用减法去做,而只要在第一个剩余数上加 $2n+1$,以后每个加数再递加2就行了.其结果如表83所示.

类似地可求得负剩余数,只要我们愿意,表可以造得很长,但由于只要求出小于250的五个剩余数,所以不需要把表格造得很长.当然,在剩余数列中的每个数都是一个平方剩余,而问题是要求出在设定上限250以下的剩余数.在表格中,小于这个上限的,只有250一数.但是,人们省悟到,若一个剩余数中含有平方数因子,则该因子可以忽略不计,而所剩者仍然是平方剩余,这是由于,平方数对任何模的平方性态总是+1.例如,若有一个剩余数 $R=a^2b$,有关的模是 N,则可记为 $(a^2|N)(b|N)=+1(b|N)=(b|N)$.应用这一规则我们发现−11与−47也是平方剩余.如把规则推广,则可得出:平方剩余的乘积仍然是平方剩余.通过明智结合,我们即有可能去掉平方因子.例如,可结合11·107与−11,即能得出−107是所求的一个平方剩余,而2·19·23与−2·13·23的结合则可得到−13·19=−247,其绝对值刚刚位于上限以下不远.到此地步,要求的五个平方剩余已经统统有了.如果想求出250以下的为数更多的平方剩余,那就有必要扩充这张表格.

[208]

n	剩余 $=R$ $=n^2-N$	剩余的因子分解	n	剩余 $=R$ $=n^2-N$	剩余的因子分解
368	137	137	367	−598	−2·13·23
369	874	2·19·23	366	−1331	−11·(11^2)
370	1613	1613	365	−2062	−2·1031
371	2354	11·107	364	−2791	−2791
372	3097	19·163	363	−3518	−2·1759
373	3842	2·17·113	362	−4243	−4243
374	4589	13·353	361	−4966	−2·13·191
375	5338	2·17·157	360	−5687	−47·(11^2)

表83 $N=135287$ 的平方剩余

在绝大多数研究中,人们只是对那些与模互质的平方剩余感兴趣;因此需对剩余列中的数一一进行检查,除非人们已经知

道模是一个素数.至于要确定两数是否互质,怎样求其最大公约数等内容,一般的算术或代数教科书中都能查到.如果这一最大公约数等于1,两数当然是互质的.

*　　*　　*

从以上所述的内容,人们也许会猜想,在一串数字中,平方剩余与平方非剩余的个数是平分秋色的.但若 p 是 $4x-1$ 形式[209]的素数,则在一串数字 $1,2,3,\cdots,(p-1)/2$ 中,平方剩余的个数要多于平方非剩余的个数.例如,若 $p=19$,则1,2,3,4,5,6,7,8,9中有六个平方剩余数:1,4,5,6,7,9.

参考文献

Bell, E. T. *Men of Mathematics*. New York: Simon and Schuster, 1937.

Dickson, L. E. *Introduction to the Theory of Numbers*. New York: Dover Publications, Inc., 1957.

Lehmer, D. N. *Factor Stencils*. Washington, D. C.: Carnegie Institution of Washington, 1939.

——. "A Photo-Electric Number Sieve," *American Mathematical Monthly*, **40**(1933), 401.

Mathews, G. B. *Theory of Numbers*. New York: Chelsea Publishing Co., 1961.

Reid, L. W. *Elements of the Theory of Algebraic Numbers*. Baltimore: Johns Hopkins Press, 1946.

Uspensky, J. V., and Heaslet, M. A. *Elementary Number Theory*. New York: McGraw-Hill Book Co., 1939.

Vinogradov, I. M. *Elements of Number Theory*. New York: [210] Dover Publications, Inc., 1954.

第20章 争攀高峰

要想编织数论的这件华服，无所不在的素数是织物的主要经纬. 几乎任何一项研究里头都有它；它是我们这栋数之大厦的基本建筑材料. 从卑微的 2（唯一的偶素数）与 1（最小的奇素数）[1]开始，它一股劲地向上无限攀升，孤芳自赏，人们对它无计可施. 几乎无法攀缘的高峰如 $(10^{23}-1)/9$ 以及一度曾经举世无匹的，39 位的数字 $2^{127}-1$ 最后终于倒下，向揭破其奥秘的人们俯伏称臣，最终都被证明为素数. 然而，目前无人能说出什么数是已知的最大素数，因为一夜之间可能就会发现一个更大者. 截至本书执笔时止，作者所知的最大素数为 $2^{11213}-1$，这一素数有 3376 位. 美国伊利诺大学的伊里亚克 Ⅰ 型数字计算机需要花费 135 分钟，进行 12 亿 2500 万次加法与乘法运算来证明此数是一个素数；如果用手算，则需要 125 个人在一起干上一千年.[2]

目前仍在昂首挺胸、睥睨众人的尚未定性的数字巨人中，究竟有哪些最终纳入我们的认识世界，判定其为素数或合数？在那些由清一色数字（从 $(10^{37}-1)/9$ 到 $(10^{97}-1)/9$，即分别由 37 个 1 与 97 个 1 所构成的数）所构成的崇山峻岭中，10 的指数为 47；59；67；71；73；83 与 89 的群峰，它们的情况究竟如何？若素

---

① 请参见第 98 页的注. ——译者注.

② 目前已发现的最大素数为 $2^{1398269}-1$，其十进形式有 40 万位，它是 1996 年 11 月发现的. ——译者注.

数的幂指数比100还大,情况又将怎样?

从数学史上的黎明时期开始,素数一直是不守规矩的"化外之民",所有想把它们分类整理的一切企图都失败了.人们徒劳无功地注视着素数表,想从中找出第n个素数与其数值之间的某种关系,即素数序列的规律,然而一次又一次地遭到挫折.上一世纪,一些伟大数学家指挥了数学解析的重武器来对付这些难以攻破的顽固堡垒,把以前只是在连续领域中应用的方法引入离散领域,有时也显示出一些惊人成果.例如,导出了一个近似公式,它能给出在一个区间内的素数个数,其准确程度令人刮[211]目相看.尽管如此,捉弄人的是,随着范围的扩展,准确度却并不是越来越好(这种情况在其他场合经常是对的),而是以随机方式振荡,完全无法作出预测.

数越变越大时,它们具有除数的概率也随之增大,人们难免设想存在一个极限,一旦逾越了这个极限,任何正整数将不可能是素数.但是,欧几里得早就用一种极其初等的办法证明素数是无限多的.由于其简洁性,这个证法几乎永远保持其魅力.

设想素数的个数并非无穷多,而p是最大的素数.令$N=2\cdot3\cdot5\cdot7\cdot\cdots\cdot p$为从2至$p$并保持其自然顺序的一切素数的乘积,$N$当然能被从2到$p$的任何一个素数整除.然而$N+1$却不能被任何一个素数除尽,因为用任一个素数去除$N+1$时,总会留下余数1.因而,只能存在以下两种可能性之一:

1. $N+1$,如果是一个合数的话,则它能被一个大于p的素数整除;

2. $N+1$不能被任何小于其本身的数整除,换言之,$N+1$是个素数.

在后一种情况,比p大得多的数$N+1$将是个素数;而在前一种情况,$N+1$的一个素因子将大于p.不论何者,这都意味着存在一个比p更大的素数,这就引出了矛盾,于是欧几里得用反证

法证明了根本不存在一个最大的素数 p.

* * *

一位希腊早期学者埃拉多塞尼(Eratosthenes)发明了一种极简单的办法用以找出并列举素数.按自然顺序写下所有的正整数.从 2 开始,每次划掉相继两数中的第二个数,但需将最初的 2 保留下来.这样继续进行下去,随便怎么长都行.再从 3 开始,每逢第三个数就把它划掉,但 3 本身要保留.然后又重头做起,从 3 后面第一个没有划掉的数 5 开始,每数到第五个数就划去.接着,又从下一个未划掉的数 7 开始,每数到第七个数就把它划去,……依此类推,不论已划去或没有划去,点数时都得考虑.这样做过以后,未划掉的数就是素数:

1,2,3,~~4~~,5,~~6~~,7,~~8~~,~~9~~,~~10~~,11,~~12~~,13,~~14~~,~~15~~,~~16~~,17,
~~18~~,19,~~20~~,~~21~~,~~22~~,23,~~24~~,~~25~~ [212]

上图表明不超过 25 的素数表是怎样通过此种方法造出来的.

也可以设想有一条长长的纸带,上面按自然顺序打印着一切正整数.它经过一台打印机,对纸带上在 2 以后的数目,每数到第二个数就把它穿孔;……纸带又经过另一台打印机,把 3 后面的数,每数到第三个就穿孔;……这样依此类推,结果留下来没有穿过孔的数便能组成一张素数表.

表 84 列出了从 1 到 55079 的前 5600 个素数.它来自雷默的 1～10000000 之间的素数表.

花费在素数表上的劳动称得上是奇迹,这种努力是为自己,丝毫也没有受到物欲的污染,以致人们在阅读这类表格时,不免升华出由衷的赞叹.L·E·狄克逊在其巨著《数论史》的第二卷里表达了这种感情,正是它鼓舞作者付出了如此艰巨的劳动.它(指素数表)"完全符合了造表者的强烈自信心;每个人都应当在其一生的某个时期干出一些重大的业绩,这些工作除了能使他

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
														1	1	1	1	1	1	1	1	1	1	2	2	2	2	2
1	1	541	1223	1987	2741	3571	4409	5279	6133	6997	7919	8831	9733	0657	1657	2553	3499	4519	5401	6381	7389	8313	9423	0357	1383	2307	3321	4281
2	2	47	29	93	49	81	21	81	43	7001	27	37	39	63	77	69	513	33	13	411	93	29	27	59	91	43	27	317
3	3	57	31	97	53	83	23	97	51	13	33	39	43	67	81	77	23	37	27	17	401	41	29	69	97	49	33	29
4	5	63	37	99	67	93	41	303	63	19	37	49	49	87	89	83	37	43	39	21	17	53	33	89	401	67	39	37
5	7	69	49	2003	77	607	47	09	73	27	49	61	67	91	99	89	53	49	43	27	19	67	41	93	07	69	57	59
6	11	71	59	11	89	13	51	23	97	39	51	63	69	709	701	601	67	51	51	33	31	71	47	99	19	81	69	71
7	13	77	77	17	91	17	57	33	99	43	63	67	81	11	17	11	77	57	61	47	43	79	57	407	33	91	71	73
8	17	87	79	27	97	23	63	47	203	57	93	87	87	23	19	13	91	61	67	51	49	97	63	11	67	97	99	79
9	19	93	83	29	801	31	81	51	11	69	8009	93	91	29	31	19	97	63	73	53	67	401	69	31	81	409	417	91
10	23	99	89	39	03	37	83	81	17	79	11	923	803	33	43	37	613	91	93	77	71	13	71	41	87	33	31	407
1	29	601	91	53	19	43	93	87	21	103	17	29	11	39	77	41	19	93	97	81	77	27	77	43	91	41	47	13
2	31	07	97	63	33	59	507	93	29	09	39	33	17	53	79	47	27	621	511	87	83	33	83	77	93	47	59	19
3	37	13	301	69	37	71	13	99	47	21	53	41	29	71	83	53	33	27	27	93	89	39	89	79	99	53	73	21
4	41	17	03	81	43	73	17	407	57	27	59	51	33	81	89	59	49	29	41	519	91	43	501	83	503	69	97	39
5	43	19	07	83	51	77	19	13	63	29	69	63	39	89	801	71	69	33	51	29	97	51	07	507	17	81	509	43
6	47	31	19	87	57	91	23	17	69	51	81	69	51	99	07	89	79	39	59	47	509	57	31	09	21	83	31	69
7	53	41	21	89	61	97	47	19	71	59	87	71	57	831	13	97	81	53	69	53	19	61	41	21	23	501	37	73
8	59	43	27	99	79	701	49	31	77	77	89	99	59	37	21	703	87	57	81	61	39	81	43	33	29	11	39	81
9	61	47	61	111	87	09	61	37	87	87	93	9001	71	47	27	13	91	69	83	67	51	93	53	43	57	31	49	99
20	67	53	67	13	97	19	67	41	99	93	101	07	83	53	31	21	93	83	601	73	69	503	59	49	59	41	57	509
1	71	59	73	29	903	27	83	43	301	207	11	11	87	59	33	39	97	99	07	603	73	17	71	51	63	43	61	17
2	73	61	81	31	09	33	91	71	11	11	17	13	901	61	39	43	709	713	19	07	79	21	77	63	69	49	63	27
3	79	73	99	37	17	39	97	77	17	13	23	29	07	67	63	57	11	17	29	19	81	23	83	93	77	67	67	33
4	83	77	409	41	27	61	603	79	23	19	47	41	23	83	67	63	21	23	41	31	97	39	97	99	87	71	81	47
5	89	83	23	43	39	67	21	83	29	29	61	43	29	89	87	81	23	31	43	33	99	41	603	611	89	73	93	51
6	97	91	27	53	53	69	37	501	37	37	67	49	31	91	97	91	29	37	47	49	609	53	09	27	99	613	99	71
7	101	701	29	61	57	79	39	03	43	43	71	59	41	903	903	99	51	41	49	51	23	83	61	39	601	19	603	93
8	03	09	33	79	63	93	43	07	53	47	79	67	49	09	09	809	57	47	61	57	27	87	81	41	11	21	09	611
9	07	19	39	203	69	97	49	19	59	53	91	91	67	37	23	21	59	53	67	61	57	93	87	63	13	37	23	23
30	09	27	47	07	71	803	51	21	61	83	209	103	73	39	27	23	63	59	71	73	59	617	97	81	17	39	27	31
1	13	33	51	13	99	21	57	27	67	97	19	09	0007	49	33	29	81	67	79	91	69	37	99	93	47	43	29	59
2	27	39	53	21	3001	23	63	31	73	307	21	27	09	57	39	41	89	71	83	93	81	61	709	707	49	51	33	71
3	31	43	59	37	11	33	73	57	79	09	31	33	37	73	41	53	99	79	727	99	83	71	17	17	61	69	63	77
4	37	51	71	39	19	47	79	63	89	21	33	37	39	79	53	89	807	83	31	703	707	79	27	19	73	79	69	83
5	39	57	81	43	23	51	91	69	97	31	37	51	61	87	59	93	29	97	33	29	13	91	39	31	83	91	71	91
6	49	61	83	51	37	53	703	73	421	33	43	57	67	93	69	99	31	813	37	41	29	701	51	43	701	97	77	97
7	51	69	87	67	41	63	21	81	27	49	63	61	69	1003	71	907	41	21	39	47	37	13	53	47	13	99	87	709
8	57	73	89	69	49	77	23	91	49	51	69	73	79	27	81	11	59	27	49	59	47	19	59	49	27	709	89	33
9	63	87	93	73	61	81	29	623	51	69	73	81	91	47	87	17	73	31	61	63	49	31	63	53	37	17	719	49
40	67	97	99	81	67	89	33	39	69	93	87	87	93	57	2007	19	77	43	67	87	61	43	77	59	39	21	41	63
1	73	809	511	87	79	907	51	41	73	411	91	99	99	59	11	23	79	51	73	811	83	49	93	71	51	27	43	67
2	79	11	23	93	83	11	59	47	81	17	93	203	103	69	37	41	83	67	87	23	89	57	801	73	57	39	47	81
3	81	21	31	97	89	17	83	51	91	33	97	09	11	71	41	53	901	69	91	29	91	73	13	89	67	41	53	93
4	91	23	43	309	109	19	87	53	521	51	311	21	33	83	43	59	03	79	97	31	807	87	19	807	73	51	61	99
5	93	27	49	11	19	23	89	57	29	57	17	27	39	87	49	67	07	87	803	43	27	93	41	09	87	69	67	809
6	97	29	53	33	21	29	93	59	47	59	29	39	41	93	71	73	13	91	09	71	37	97	43	49	99	77	73	21
7	99	39	59	39	37	31	99	69	51	77	53	41	51	113	73	79	21	97	17	79	39	803	53	57	803	83	89	41
8	211	53	67	41	63	43	801	83	53	81	63	57	59	17	97	83	31	923	23	83	51	39	61	73	17	87	801	47
9	23	57	71	47	67	47	13	89	63	87	69	77	63	19	101	3001	33	29	59	89	63	59	67	79	21	807	13	51
50	27	59	79	51	69	67	17	89	69	89	77	81	69	31	07	03	63	39	77	901	81	69	89	87	39	11	19	59

表 84 素数表[1]

① 本表复印自 D·N·雷默著,《因数模板》,第二版,第 14~15 页,原书由华盛顿卡内基学院于 1939 年出版.此事已征得有关方面的同意.——原注.

表 84 素数表(续)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
														1	1	1	1	1	1	1	1	1	1	2	2	2	2	2
51	29	43	63	67	81	69	31	93	71	99	87	83	77	49	09	07	87	47	61	03	91	09	91	97	41	17	27	77
2	33	77	97	71	87	4001	61	701	77	907	89	93	83	69	13	09	97	51	67	21	903	911	913	99	61	33	31	89
3	39	81	601	77	91	03	71	11	81	17	419	311	93	81	19	33	99	57	89	27	09	13	19	803	69	39	33	907
4	41	83	07	81	203	07	77	17	99	23	23	19	211	71	43	37	4003	69	901	31	11	17	27	21	63	61	57	17
5	51	87	09	83	09	13	89	27	807	29	29	23	23	73	49	43	11	93	07	37	21	19	37	29	71	71	69	19
6	57	907	13	89	17	19	903	41	29	37	31	37	43	77	67	49	29	3013	13	43	23	47	49	39	81	77	73	29
7	63	11	19	93	21	21	09	43	37	41	43	41	47	87	81	63	33	17	19	63	29	69	61	47	83	901	79	43
8	69	19	21	99	29	27	19	49	53	47	47	43	53	213	83	93	51	31	23	79	39	73	63	59	911	07	87	53
9	71	29	27	411	31	49	31	79	69	49	61	49	69	39	97	99	57	33	37	81	67	79	73	63	29	21	93	67
60	77	37	37	17	63	61	33	83	41	59	67	71	87	43	203	103	71	61	39	87	89	1001	79	81	37	37	99	71
1	81	41	67	23	67	67	37	91	73	61	601	77	73	51	11	09	81	73	71	93	71	09	91	83	43	43	909	77
2	93	47	63	37	89	73	43	801	79	73	13	91	79	67	27	21	83	77	73	7011	77	13	93	1001	61	61	11	79
3	99	63	87	41	71	79	61	07	89	77	21	97	89	61	39	27	87	83	91	21	81	31	97	11	77	63	17	89
4	307	67	69	47	99	81	67	13	91	83	27	403	301	73	41	47	107	91	6001	27	87	37	0011	13	91	73	29	3013
5	11	71	93	59	301	93	87	31	701	89	37	13	03	79	61	51	43	101	07	29	89	51	21	17	97	93	37	31
6	13	77	97	67	07	99	69	37	03	91	39	19	13	87	33	59	49	07	33	33	4013	69	23	19	2003	5003	71	33
7	17	83	89	73	13	111	73	39	09	403	43	21	21	99	63	63	53	21	37	41	41	73	29	23	13	11	77	37
8	31	91	709	77	19	27	87	43	19	07	63	31	31	311	89	71	89	31	61	47	43	79	47	31	27	17	81	57
9	37	97	21	803	23	29	93	49	13	21	73	39	33	17	77	77	73	37	63	53	47	81	51	59	31	21	83	73
70	47	1009	23	21	39	33	99	51	37	39	81	57	37	21	81	83	77	39	67	77	49	87	63	61	37	27	4001	87
1	49	13	33	31	31	39	5003	57	61	43	97	39	49	29	99	87	97	49	69	93	59	121	71	67	39	29	07	97
2	83	19	41	39	43	63	09	61	63	49	99	61	67	51	301	517	207	61	73	99	61	39	89	89	51	39	19	111
3	89	31	47	43	47	67	11	67	79	69	609	63	69	53	23	19	21	73	87	107	77	41	101	101	65	41	23	17
4	87	51	53	49	59	69	21	69	81	73	23	67	91	69	29	29	43	87	91	17	89	57	07	07	67	53	29	21
5	73	53	59	61	61	77	23	79	91	81	29	73	99	83	43	41	49	93	97	23	97	63	13	21	73	57	43	27
6	79	39	77	57	71	201	39	81	93	87	29	79	417	93	47	49	51	99	103	37	119	81	17	39	79	59	49	47
7	83	49	83	79	73	11	81	97	803	91	41	91	29	99	73	59	81	217	11	59	21	83	23	43	91	63	61	53
8	89	51	87	91	89	17	59	803	23	99	47	97	33	411	77	67	93	27	27	67	27	207	29	49	93	71	71	63
9	97	61	89	93	91	19	77	25	27	703	63	511	53	23	79	91	303	33	39	83	31	11	43	57	109	81	77	69
80	401	63	801	409	407	29	81	27	29	17	69	21	97	37	91	97	21	41	41	89	33	13	47	63	11	87	83	71
1	09	89	11	17	13	31	87	39	33	23	77	33	59	43	401	309	23	59	83	91	43	29	49	69	23	99	91	83
2	19	87	23	21	33	41	99	53	41	27	81	39	63	47	09	13	27	63	87	203	49	31	61	79	29	117	97	89
3	21	91	31	33	49	43	101	81	57	41	89	47	77	67	13	27	41	69	89	07	69	37	73	87	33	31	103	219
4	31	93	47	47	87	63	07	87	63	53	93	51	87	71	21	31	47	71	93	09	81	49	77	91	47	43	07	29
5	33	97	61	57	61	69	13	6007	69	57	99	87	99	83	33	37	69	77	217	31	91	59	83	93	53	59	09	37
6	39	103	67	69	63	61	19	11	71	59	707	601	501	89	37	59	67	87	23	39	99	67	201	211	57	67	13	43
7	43	09	71	83	67	71	47	29	83	89	13	13	13	91	51	47	69	89	29	67	211	73	19	21	59	73	21	47
8	49	17	73	71	69	73	53	37	99	93	19	19	29	97	57	61	401	99	31	91	17	89	31	27	71	89	33	53
9	67	23	77	77	91	83	67	43	907	817	31	23	31	503	73	97	07	307	49	93	25	301	33	47	89	97	37	61
90	41	29	79	83	99	89	71	67	11	23	37	29	59	19	79	99	11	13	53	99	29	09	49	69	93	301	51	301
1	83	51	89	87	511	97	79	53	17	29	41	31	67	27	87	411	19	19	67	317	33	19	61	77	229	03	69	03
2	67	53	901	89	17	327	89	67	47	41	47	43	89	49	91	17	23	29	73	21	51	33	69	83	47	09	79	07
3	79	63	07	93	27	37	97	73	49	53	53	49	97	51	97	21	31	31	301	27	53	73	87	313	59	27	81	09
4	87	71	13	99	29	39	209	79	59	67	61	61	601	79	503	41	37	49	19	35	57	79	97	17	71	51	97	21
5	91	81	31	707	33	49	27	89	61	73	79	77	07	87	11	51	47	59	35	41	69	81	323	19	73	49	203	39
6	99	87	33	11	39	57	31	91	67	77	83	79	13	93	17	57	49	61	39	51	87	87	27	23	77	79	23	43
7	503	93	49	13	41	63	33	101	71	79	603	89	27	97	27	63	61	73	49	59	89	91	33	41	79	91	29	49
8	09	801	51	19	47	73	37	13	77	83	07	97	31	617	39	69	79	77	61	77	301	403	41	47	83	93	39	57
9	21	13	73	29	57	81	61	21	83	901	19	719	39	21	41	77	89	83	63	83	07	17	47	77	91	97	47	67
100	23	17	79	31	59	87	73	31	91	07	21	21	51	33	47	87	503	91	69	87	11	21	53	79	303	311	51	73
													1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2

	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	5	5	5	5
1	5381	6399	7449	8499	9443	0539	1601	2609	3613	4649	5739	6781	7813	8821	9971	1081	2073	3051	4201	5307	6447	7527	8611	9663	0753	1803	2919	3993
2	409	407	57	513	53	77	07	11	17	51	71	87	31	23	79	113	83	43	03	17	51	33	19	67	47	17	37	4003
3	11	17	79	17	73	93	27	21	19	67	97	91	47	33	83	17	89	67	07	19	57	43	23	69	73	27	31	11
4	23	23	81	37	83	631	43	33	23	73	801	93	53	53	89	31	101	93	21	29	71	63	47	81	77	29	57	13
5	39	31	87	41	501	37	49	47	29	79	03	809	61	59	0009	41	31	103	49	37	77	69	49	97	89	39	63	37
6	47	37	509	47	27	43	57	53	37	87	09	21	71	71	13	43	39	17	57	41	89	81	61	711	821	53	67	49
7	53	49	27	49	31	49	63	87	41	93	31	33	79	77	31	49	57	33	63	43	99	91	73	27	33	59	73	59
8	57	59	29	59	37	61	67	93	47	703	37	47	89	93	37	61	69	51	67	61	507	99	77	39	39	69	81	63
9	63	79	39	71	47	71	87	707	79	21	39	57	97	9019	39	77	79	59	69	77	11	609	79	41	49	71	99	91
10	69	89	41	73	69	77	99	13	703	29	51	71	907	23	61	79	81	77	73	89	23	23	731	47	57	93	3003	101
1	71	97	61	79	73	89	721	17	13	39	63	77	31	41	67	83	87	89	79	403	49	29	33	57	67	99	17	21
2	523	501	81	91	81	97	23	19	21	47	69	87	37	43	93	89	93	201	81	13	59	39	51	63	73	907	47	33
3	37	13	83	97	87	703	27	49	39	57	79	89	43	47	99	201	97	07	93	27	67	53	67	87	91	13	51	39
4	41	39	611	603	99	07	29	71	49	59	87	901	47	79	111	03	209	23	351	33	73	57	61	89	93	29	69	51
5	43	47	19	07	611	13	41	79	51	63	99	13	67	89	23	13	21	37	87	39	89	59	67	801	909	41	77	63
6	77	61	31	19	29	27	51	83	57	81	911	19	91	97	27	21	23	61	71	81	91	81	79	07	23	49	87	67
7	79	73	47	21	33	57	69	89	67	807	23	23	93	103	29	27	27	71	81	91	601	99	81	11	29	71	89	81
8	89	91	53	27	41	63	71	97	69	19	33	29	97	07	51	31	39	83	83	97	19	701	87	23	51	73	93	93
9	99	97	73	31	63	73	93	801	73	41	51	31	8011	13	53	33	57	91	89	503	33	11	99	31	57	77	101	217
20	601	617	89	49	69	81	99	03	91	43	63	43	39	19	63	43	81	313	417	23	39	13	809	43	69	91	13	31
1	03	33	91	49	71	803	817	31	97	47	69	47	47	33	69	57	83	19	49	33	43	17	17	53	71	2009	17	49
2	09	41	97	57	83	09	47	33	809	49	77	73	53	39	77	63	93	21	59	41	49	37	21	71	89	21	29	77
3	21	47	701	61	717	17	49	39	11	71	83	79	69	57	89	69	99	31	83	53	63	41	23	77	93	27	47	87
4	33	69	33	63	23	29	59	43	37	77	93	97	83	61	93	81	307	61	91	57	79	43	47	91	1001	51	49	93
5	39	81	37	69	41	39	73	69	39	83	99	1003	113	63	213	99	23	97	97	89	81	77	57	919	31	57	61	311
6	43	83	39	87	53	41	83	87	51	97	4007	13	19	81	31	333	31	99	501	87	87	79	59	21	43	67	71	19
7	57	87	43	97	69	61	91	909	57	913	11	19	49	91	37	41	37	403	07	89	91	91	69	27	47	69	73	23
8	67	93	49	703	61	83	907	11	63	19	13	21	83	99	41	51	47	11	19	99	703	97	71	37	59	81	89	31
9	73	99	51	11	89	89	97	17	71	39	17	39	87	209	53	87	59	27	31	613	25	807	83	39	61	103	97	47
30	79	701	63	23	803	99	63	33	89	49	37	49	77	17	77	81	73	41	33	31	27	09	89	43	71	21	201	61
1	93	11	67	29	19	71	73	59	93	61	61	57	83	27	83	87	79	51	37	41	47	19	907	57	109	27	31	67
2	703	13	73	31	33	81	81	41	911	63	87	41	89	39	89	89	91	49	43	89	51	37	47	91	31	47	33	71
3	17	17	79	53	37	93	91	57	23	81	93	87	97	33	343	99	97	61	49	87	57	43	53	93	33	53	39	77
4	39	33	91	59	51	911	2003	69	51	5023	83	97	801	39	51	411	403	67	63	73	69	57	73	99	37	63	67	401
5	41	39	93	71	63	31	09	71	97	37	97	117	19	41	97	13	07	99	79	77	71	69	89	0021	41	77	69	03
6	47	51	99	89	67	37	27	83	41	51	107	23	31	51	61	43	09	317	87	81	807	81	91	23	57	81	79	09
7	59	37	803	83	73	41	29	87	61	53	09	39	37	93	67	53	33	41	617	97	11	903	9003	33	69	83	81	13
8	63	59	09	807	79	49	51	93	67	59	51	59	39	301	423	67	37	43	21	707	17	11	09	47	93	89	99	19
9	71	77	17	13	81	71	87	99	87	69	37	71	61	13	27	79	43	73	33	37	19	17	19	51	97	201	309	21
40	93	83	23	17	917	77	89	3013	4019	81	81	81	73	17	29	91	91	77	33	31	29	33	31	53	99	23	23	37
1	99	801	87	37	21	83	83	23	31	83	81	89	81	23	33	307	87	79	41	67	31	39	33	69	203	37	27	43
2	801	13	47	43	27	1013	89	29	33	89	87	99	87	41	59	13	61	91	47	83	53	67	37	77	17	49	43	49
3	19	21	51	89	47	19	77	37	39	99	91	201	99	43	71	19	63	97	61	67	61	51	43	87	29	83	59	69
4	41	33	83	67	59	23	83	49	37	107	209	17	303	59	83	21	67	407	57	79	67	43	57	93	39	59	77	93
5	47	39	93	71	63	39	97	53	41	11	17	39	17	67	87	39	73	09	83	617	77	69	49	101	41	67	81	97
6	49	49	901	79	69	51	99	71	123	17	39	43	21	71	93	43	87	13	87	21	89	77	81	11	57	89	401	99
7	87	61	17	901	9011	63	117	73	27	29	41	53	27	73	99	49	91	27	99	23	901	81	103	19	63	91	07	603
8	73	63	19	09	19	69	19	83	29	41	51	73	29	83	507	79	99	33	701	27	19	9017	09	23	83	301	11	17
9	89	79	41	21	29	79	41	91	41	49	63	77	33	87	19	83	509	49	11	33	33	23	17	29	87	13	19	21
50	903	81	43	27	47	81	43	107	47	53	69	307	61	409	29	87	33	51	29	41	87	29	21	31	307	21	37	39

表 84 素数表(续)

	29	30	31	32	33	34	35	36	37	38	39	40	41	42
	1	2	2	2	2	3	3	3	3	3	3	3	3	3
51	13	91	47	33	69	91	39	13	67	19	77	09	71	19
2	19	93	53	49	71	121	73	19	69	71	83	13	77	39
3	31	903	61	61	89	23	83	49	71	301	89	21	93	49
4	33	21	67	79	91	39	89	61	83	21	307	37	431	61
5	39	27	83	3001	97	47	91	91	811	27	13	39	47	81
6	43	47	97	19	103	51	303	79	13	61	19	57	49	99
7	61	51	8001	21	07	53	13	83	19	67	41	61	53	803
8	69	63	19	33	13	69	23	91	31	47	43	63	59	09
9	81	69	27	37	19	77	27	99	53	79	53	69	81	11
60	97	91	31	43	33	81	41	201	69	81	73	79	501	21
1	99	97	51	39	37	83	47	11	41	91	83	97	43	41
2	4003	99	57	43	39	89	61	33	87	311	89	409	57	51
3	19	7011	69	77	61	93	77	47	73	17	433	23	61	53
4	21	17	81	101	69	219	99	87	83	23	51	41	77	69
5	29	31	87	33	81	23	303	89	97	37	57	47	99	81
6	41	43	97	39	87	31	09	301	801	39	67	63	93	907
7	53	49	99	51	97	37	21	11	03	63	69	83	603	19
8	59	61	109	57	303	47	33	17	13	69	73	89	09	23
9	89	67	11	47	11	49	27	29	19	81	79	93	11	31
70	107	73	23	63	23	53	41	31	27	93	83	501	29	39
1	11	77	51	67	41	59	53	43	37	401	97	07	39	57
2	13	91	63	73	53	67	59	49	51	07	823	11	51	71
3	19	103	81	79	59	71	63	59	61	19	37	17	53	79
4	41	07	83	91	69	77	69	63	67	23	39	29	59	703
5	53	09	201	201	71	307	71	89	89	37	41	37	71	09
6	61	27	11	07	93	19	77	77	81	47	51	47	77	19
7	71	43	19	09	307	21	81	91	403	49	59	49	93	27
8	77	79	29	21	13	27	401	403	21	61	63	61	99	33
9	83	91	77	31	19	33	11	09	29	81	71	67	707	49
80	89	97	79	43	23	37	13	13	39	807	83	71	11	61
1	903	311	83	41	41	57	23	27	57	09	87	73	13	69
2	09	39	89	69	47	79	59	37	69	21	99	79	23	79
3	27	41	97	87	67	87	41	81	71	27	907	89	29	91
4	37	53	307	97	89	91	43	89	83	31	29	91	37	99
5	49	59	09	303	91	93	67	99	87	39	37	607	47	921
6	51	71	19	11	403	97	79	87	99	57	43	19	49	27
7	61	77	49	27	27	469	91	93	901	43	53	23	67	29
8	63	81	51	33	31	77	97	503	11	69	71	43	83	39
9	67	83	57	39	49	81	503	21	13	73	77	49	91	41
90	93	99	93	47	47	89	07	29	19	91	83	57	803	47
1	97	329	403	63	69	511	31	33	37	93	91	63	21	57
2	909	37	09	83	81	13	33	47	43	97	97	91	33	63
3	17	41	11	87	95	17	37	63	49	603	709	93	39	69
4	21	67	29	89	97	31	61	69	63	17	13	99	51	77
5	39	97	33	99	509	41	63	77	89	71	21	717	61	83
6	47	407	39	401	17	43	69	81	91	77	39	47	67	87
7	57	09	47	11	29	47	73	87	903	729	49	81	73	901
8	71	27	63	23	39	67	79	89	07	31	61	83	91	29
9	87	31	77	29	53	73	87	99	13	47	67	99	903	37
100	93	37	93	37	57	83	603	601	31	53	79	811	17	53
	2	2	2	2	3	3	3	3	3	3	3	3	3	3

	43	44	45	46	47	48	49	50	51	52	53	54	55	56
	3	4	4	4	4	4	4	4	4	4	5	5	5	5
51	31	803	67	41	41	93	93	69	23	47	29	61	41	41
2	43	09	69	49	53	83	97	73	39	53	41	63	53	47
3	69	11	71	91	71	89	7017	79	57	59	43	67	79	59
4	77	17	77	711	73	87	41	91	69	77	47	79	503	63
5	83	21	89	17	77	93	81	109	71	207	49	87	07	77
6	91	27	611	21	99	943	67	19	77	21	61	91	27	81
7	97	41	41	53	97	49	69	21	93	27	83	433	49	83
8	909	47	43	59	909	53	87	31	99	31	407	53	51	601
9	27	51	49	77	19	59	93	37	201	61	13	57	69	17
60	37	59	67	81	39	71	111	43	07	83	19	89	91	23
1	59	69	77	83	43	79	19	79	11	73	21	501	93	29
2	93	81	83	87	51	89	23	87	23	87	27	11	97	31
3	97	87	89	89	67	8021	29	93	53	91	31	17	609	47
4	99	719	97	93	79	29	37	97	61	311	37	29	11	67
5	709	29	701	801	87	49	43	221	77	33	39	41	17	73
6	39	37	03	33	93	51	47	39	79	29	49	43	23	79
7	51	39	09	47	909	61	49	47	97	33	61	53	29	709
8	59	41	19	49	17	73	61	59	307	41	73	61	33	13
9	63	71	27	81	27	91	89	71	31	59	79	67	39	21
70	71	77	37	913	39	93	207	81	33	63	81	71	53	27
1	87	801	43	33	53	99	21	99	39	77	87	79	57	61
2	801	09	51	43	59	103	37	311	63	83	503	83	81	67
3	13	13	67	51	83	33	51	13	67	87	11	609	93	73
4	19	43	73	61	71	41	69	37	69	411	17	27	99	79
5	23	49	87	63	83	47	79	41	91	17	21	31	717	87
6	29	61	93	69	87	53	87	53	93	23	39	39	19	99
7	41	63	97	73	5007	71	93	71	409	41	51	67	31	829
8	47	79	821	87	13	81	97	83	11	59	63	73	59	33
9	49	87	29	91	43	83	303	97	17	81	77	91	73	51
80	53	93	39	97	61	87	09	407	29	97	81	97	77	69
1	67	97	41	4017	77	99	17	09	33	503	93	709	83	77
2	79	903	53	21	83	219	39	13	51	13	99	11	91	81
3	83	11	59	27	119	29	51	37	59	27	607	21	813	907
4	97	27	83	39	21	37	53	49	63	39	13	27	19	17
5	903	41	99	41	27	41	83	63	77	43	31	33	31	19
6	27	47	901	53	31	71	81	73	81	49	37	47	49	41
7	33	53	23	59	37	73	87	79	99	51	47	57	57	49
8	39	57	29	71	39	79	89	81	523	81	59	69	61	59
9	49	59	37	87	41	301	407	87	29	87	73	83	81	73
90	61	69	43	89	79	07	17	91	31	91	79	807	87	79
1	73	81	53	101	81	09	19	97	37	93	83	13	91	83
2	93	83	61	11	91	27	31	523	47	99	91	17	97	5001
3	1011	99	67	19	97	37	41	27	49	627	713	37	99	09
4	17	2013	79	23	233	49	59	33	59	47	19	39	917	21
5	23	17	89	29	47	51	91	39	97	61	21	61	23	49
6	39	19	3003	31	59	81	97	41	603	71	49	79	27	51
7	47	23	13	39	63	99	501	63	13	83	67	83	39	57
8	51	43	19	71	81	411	07	71	27	707	69	89	51	61
9	57	61	37	79	89	39	13	89	33	23	87	901	59	73
100	77	71	49	89	93	41	21	93	39	41	97	03	87	79
	4	4	4	4	4	4	4	4	4	5	5	5	5	5

表 84 素数表(续)

自我满意之外，极不可能会因此而获得任何酬报.”

有关纪录可以追溯到公元1202年，那时有个名叫李奥那多·皮萨诺(Leonardo Pisano)的人造出了从11到97的素数表，还编出一张12到100的合数表. 1603年，彼得罗·卡塔尔迪(Pietro Cataldi)印出一张800以下的因数表，以及750以下的素数清单. 计算家们接踵而起，把上限不断向前推进. 在表85中，我们给出了一些重要计算家的姓氏以及他们的计算范围.

编造者	年代	上限 因数表	上限 素数表
L. Pisano	1202	100	97
P. Cataldi	1603	800	750
F. van Schooten	1657		10000
J. H. Rahn	1659	24000	
T. Brancker	1668	100000	
J. G. Kruger	1746		100999
J. H. Lambert	1770		102000
A. F. Marci	1772		400000
A. Felkel	1776	408000	
A. Felkel	1785	2856000	
L. Chernac	1811	1020000	
J. C. Burckhardt	1814	1000000 至 2000000	
J. C. Burckhardt	1816	2000000 至 3000000	
J. C. Burckhardt	1817	1 至 1000000	
Z. Dase	1862	7000000 至 8000000	
Z. Dase 与 H. Rosenberg	1863	8000000 至 9000000	
J. P. Kulik	1867	1 至 100000000	
J. Glaisher	1879	3000000 至 4000000	
J. Glaisher	1880	4000000 至 5000000	
J. Glaisher	1883	5000000 至 6000000	
D. N. Lehmer	1909	1 至 10000000	
D. N. Lehmer	1914		1 至 10000000

表85 因数表与素数表

凝视着这些心血结晶时，人们不禁会生发出沉思冥想，在这样一个战乱频仍，动荡不安的世界里，心甘情愿地消磨一生

的大部分时光从事于这样一种工作的人，他们一定发现了导致内心平静安乐的秘密，这是所有的人都在追求而急功近利之徒从来未能得到的东西. 在这些工作中也显示了造表者的希望与随之而起的生活中的挫折与不幸. 例如，安东尼奥·斐凯尔(Antonio Felkel)，他在1776年完成了2000000以下，一切自然数分解为质因数的工作. 讫于408000的表的第一部分找不到买主，除了少数几本幸免厄运外，全部印出来的书都被低价抛售，在土耳其战争中买了军火！维也纳的皇家金库曾经资助过书的编印，获得并保存了作者的大部分手稿，可是后来斐凯尔未能收回其手稿，他只好把408000到2856000的数的因子重新再计算一遍！ [213]

数学家伦伯特(Lambert)曾许愿，编出1000000以下自然数因子表的人定可获得不朽美名. 兴登堡(C. F. Hindenburg)也是促进者之一，在他手里完成了这一表格. 蒲克哈特(Burckhardt)，格莱歇(Glaisher)，柯立克(Kulik)以及数学奇才戴斯(Dase)干了最主要的工作，正是在他们努力的基础上编出了现代的表格. 对美国读者来说，伸手可及的是D·N·雷默的煌煌巨著《首批一千万数的因数表》以及《1到10006721的素数表》.

柯立克的重大工作，一千万个数的因数表简直令人难以想象. 这个人把他一生中的二十年光阴完全扑在上面，全然单干，毫无帮助. 人们在阅读D·N·雷默的《因数表》的引言时也许能分享到他的一份激动心情，其时他在维也纳皇家学院里仔细审阅记载着柯立克成果的八大卷手稿的第一部分. 然而，也许是神祇们的存心捉弄，瞧不起弱者的劳动，我们了解到载有12642600到22852800的因数分解的表格不幸丢失了. 谁应对此负责？是疏忽的管理人，漫不经心的女清洁工，还是鬼头鬼脑的学生？ [218]

* * *

存在着一些很有趣的公式，对变量的许多次连续取值，它们

都能得出素数，然而，或迟或早，总是要得出合数的. 劝告学生们不要根据普通常识(而不是通过数学归纳法)仓促作出结论的一个精采例子是 x^2+x+41 这个公式. 当 x 从 0 取到 39 时，这个二次函数总是能得出素数，但当 $x=40$ 时，答数 1681 却是合数. 40 个连续素数以及其后出现的不规则情况令人注目，它们理应在此享有一席地位. 请看表 86.

x	x^2+x+41	性质*
0	41	P
1	43	P
2	47	P
3	53	P
4	61	P
5	71	P
6	83	P
7	97	P
8	113	P
9	131	P
10	151	P
11	173	P
12	197	P
13	223	P
14	251	P
15	281	P
16	313	P
17	347	P
18	383	P
19	421	P
20	461	P
21	503	P
22	547	P
23	593	P
24	641	P
25	691	P
26	743	P
27	797	P
28	853	P
29	911	P
30	971	P
31	1033	P
32	1097	P
33	1163	P
34	1231	P
35	1301	P
36	1373	P
37	1447	P
38	1523	P
39	1601	P
40	1681	C
41	1763	C
42	1847	P
43	1933	P
44	2021	C
45	2111	P
46	2203	P
47	2297	P
48	2393	P
49	2491	C
50	2591	P
51	2693	P
52	2797	P
53	2903	P

[219]

* P 代表素数，C 代表合数.

表 86 得出素数的公式 x^2+x+41

x	x^2+x+41	性质*	x	x^2+x+41	性质*
54	3011	P	78	6203	P
55	3121	P	79	6361	P
56	3233	C	80	6521	P
57	3347	P	81	6683	C
58	3463	P	82	6847	C
59	3581	P	83	7013	P
60	3701	P	84	7181	C
61	3823	P	85	7351	P
62	3947	P	86	7523	P
63	4073	P	87	7697	C
64	4201	P	88	7873	P
65	4331	C	89	8051	C
66	4463	P	90	8231	P
67	4597	P	91	8413	C
68	4733	P	92	8597	P
69	4871	P	93	8783	P
70	5011	P	94	8971	P
71	5153	P	95	9161	P
72	5297	P	96	9353	C
73	5443	P	97	9547	P
74	5591	P	98	9743	P
75	5741	P	99	9941	P
76	5893	C	100	10141	P
77	6047	P			

* P 代表素数，C 代表合数.

表 86 得出素数的公式 x^2+x+41（续）

这个公式是很突出的，作为其标志的是下列事实，如果存在着另一整数 b，使对连续 $b-1$ 个 x 值，公式 x^2+x+b 都能得出素数，则 b 必须超过 1,250,000,000，而且，至多只存在这样一个整数.

x 从 -40 取到 -1 时，同样也能得出素数，但仅不过是同样数集的重复，位移一步而已. 若用 $(x-40)$ 替代 x，则我们得出公式 $x^2-79x+1601$，它所产生的素数仍旧同上面一样，但是 80 个相继出现的素数（其中不同的素数只有 40 个）不需要依赖于

x 的负数值了.

表 87 中给出了一些所谓的素数公式以及变量之值小于 100 时,此等公式得不出素数的"失败"情况.可以看到,在任意指定的限制数 100 以内,公式 $x^2-79x+1601$ 的"效益"最佳,只有五个 x 值得出合数.

公式 $f(x)$	使 $f(x)$ 给出合数的、小于 100 的 x 值	使 $f(x)$ 给出合数的 x 值的个数
$x^2-79x+1601$	80,81,84,89,96	5
x^2+x+41	40,41,44,49,56,65,76,81,82,84,87,89,91,96	14
$2x^2+29$	29,30,32,35,39,44,50,57,58,61,63,65,72,74 76,84,87,88,89,91,92,94,95,97,99	25
$6x^2+6x+31$	29,30,31,34,36,41,44,51,55,59,61,62,64,66,69,76,80,84,86,87,88,92,93,97,99	25
$3x^2+3x+23$	22,23,27,30,38,43,44,45,46,49,51,55,56,59,62,66,68,69,70,78,85,87,88,89,91,92,95,96	28

表 87 得出素数的公式

这种类型的其他公式尚有:x^3+x^2+17,它能对 $x=-14$,-13,…,$+10$ 给出素数;$x^2-2999x+2248541$,它能对 x 从 1460 到 1539 得出 80 个素数(包括首、尾两数在内);较简单的 [220] 公式则有 x^2+x+11 与 x^2+x+17.

* * *

等差数列的各项都是素数也有实例,但项数有限.读者们当能回忆得起,在一个等差数列中,相继两项之差为一常数.表 88 中给出了一些由素数形成的等差数列的实例.

(1)	(2)	(3)	(4)	(5)	(6)
7	107	7	47	71	199
37	137	157	257	2381	409
67	167	307	467	4691	619
97	197	457	677	7001	829
127	227	607	887	9311	1039
157	257	757	1097	11621	1249
		907	1307	11931	1459
					1669
					1879
					2089

表 88 由素数组成的等差数列

[221]

* * *

素数甚至可以是回文数(顺读与倒读都一样的数);而且回文素数也能组成等差数列.下面列出四个这样的数列,而每个等差数列都由四个回文素数组成:(13931,14741,15551,16361);(10301,13331,16361,19391);(70607,73637,76667,79697);(94049,94349,94649,94949).它们的公差分别为 810;3030;3030;300.

* * *

尽管素数的个数无限,人们却能在正整数的自然序列中轻而易举地找到不含素数的任意长的区间.公式 $1\cdot2\cdot3\cdot\cdots\cdot n+A$ 可用于此项目的,n 可以是我们喜欢取的任何数值,譬如说,十亿.当 A 相继取 $2,3,4,\cdots,n$ 时,由此产生的 999999999 个连续正整数(这些数值的开路先锋是 $1,000,000,000!+2$)分别能被 $2,3,4,\cdots,n$ 整除,因而在此区间中根本不可能有任何素数.当然,$1,000,000,000!+A$ 是相当可怕的数集;然而它们是满足条件的.

只要令 $n=7$,我们就可算出 $n!=5040$;而 5042,5043,5044,5045,5046,5047 全都是合数.碰巧 5041 也是个合数,大于 5047 的数中,5048,5049,5050 也全是合数,但它们不像 5042 到 5047 六个整数,不能由公式得出.

*　　　*　　　*

表 89 给出了一些小于指定上限的素数个数的对比情况，其中之一是实际清点的结果，另一是前面曾经提到过的近似公式。这个公式记为 $\int_2^x \frac{dt}{\ln t}$，称为"$x$ 的对数积分"，或者叫做"x 的积分对数"，并简记为 $\mathrm{Li}(x)$。对不熟悉积分记号的读者，我们只要说一下，$\mathrm{Li}(x)$ 近似地等于级数

$$x\left[\frac{1}{\ln x}+\frac{1!}{(\ln x)^2}+\frac{2!}{(\ln x)^3}+\frac{3!}{(\ln x)^4}+\cdots+\frac{(n-1)!}{(\ln x)^n}\right]$$

的 n 项和就行了，当然要假设 x 与 n 都是很大的数。$\ln x$ 或 $\ln t$ 表示 x 或 t 关于底 e 的对数。这是 $\log_e x$ 或 $\log_e t$ 的现代记号。切勿把 $\ln x$ 与 $\mathrm{Li}(x)$ 搞混。

区间 x	在此区间内的素数个数 N	$\mathrm{Li}(x)=\int_2^x \frac{dt}{\ln t}$	误差 $\mathrm{Li}(x)-N$
50000	5134	5167	33
100000	9593	9630	37
200000	17985	18036	51
300000	25998	26087	89
400000	33861	33923	62
500000	41539	41606	67
600000	49099	49173	74
700000	56544	56645	101
800000	63952	64037	85
900000	71275	71362	87
1000000	78499	78628	129
1500000	114156	114263	107
2000000	148934	149055	121
2500000	183073	183245	172
3000000	216817	216971	154
4000000	283147	283352	205
5000000	348514	348638	124
6000000	412850	413077	227
7000000	476649	476827	178
8000000	539778	540000	222
9000000	602490	602676	186
10000000	664579	664918	339
100000000	5761455	5762209	754
1000000000	50847534	50849235	1701

[223]　　表 89　指定区间内的素数个数

表 89 证实了本章开头时讲过的一句话，准确度既非连续不断地递增，亦非递减，而是在杂乱无章地变动. 从表中可以看到 [222] Li(x)恒大于 N，这已被数以百万计的事例所证实. 然而，基于严格证明而非来自经验归纳的重要性再度在此表显出强大威力. 现已证明，对于充分大的 x 值，有无限多次可使 Li(x)小于 N，不过，这个所谓"充分大"的 x 值，远远超出了已有因数分解表的上限. 另外，仍然还是有无限多个实例，可使 Li(x)大于 N.

若 A 很大而 b 较小，另外还有一个近似公式可以相当准确地得出 A 到 $A+b$ 区间内的素数个数. 这个公式是：$N=b/\ln A$. 若 $A=10000000$，$b=5000$，由此将得出 $N=5000/7\ln 10=(5000/7)\log_{10}e=310.21$. 实际上在此区间内有 305 个素数.

E・梅塞尔(Meissel)当真地计算了小于十亿的素数个数，结果共有 50847479 个. 但正确答案是 50847534.

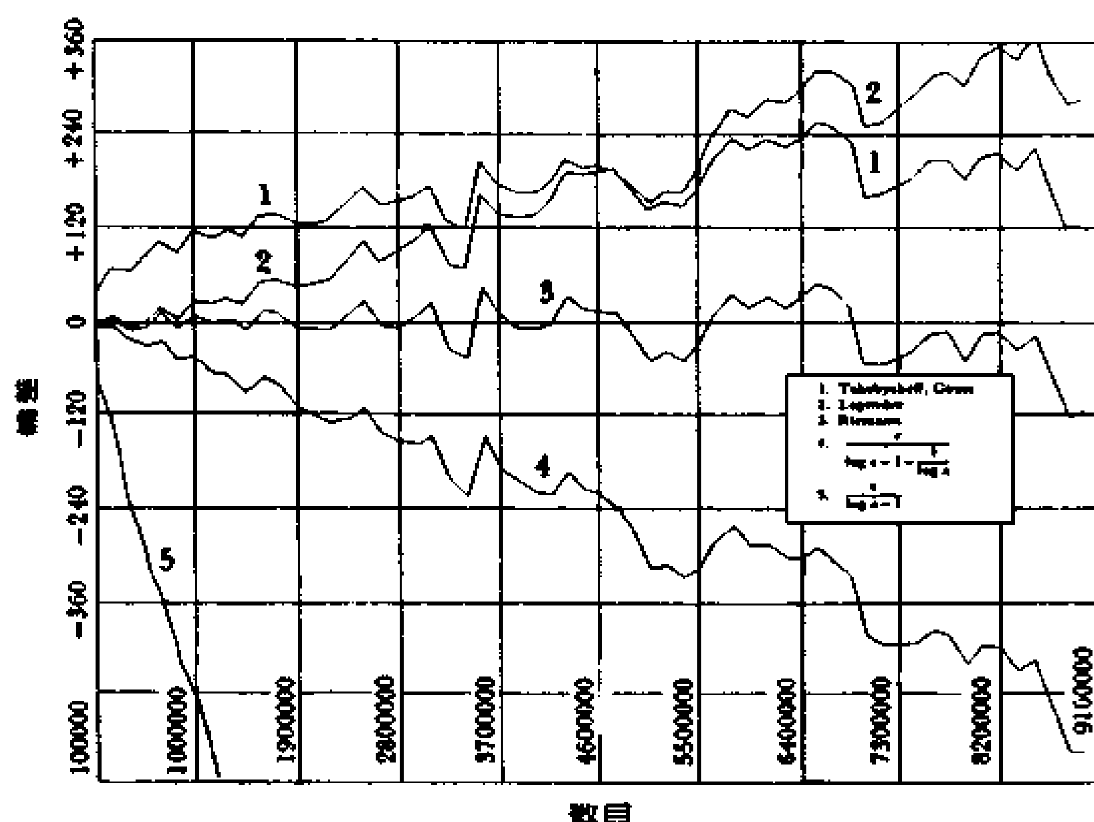


图 20 素数公式的偏差

一些研究家找到了几个极为巧妙的近似公式.图 20 的曲线显示了迄于 9000000 为止的结果对比.表 90 则给出这些公式的发明人与结果.

序号	发现者	近似公式
1	切比雪夫(Tchebycheff),高斯	$\mathrm{Li}(x)=\int_2^x \frac{dt}{\ln t}$
2	勒让德	$x/(\ln x-1.08366)$
3	黎曼(Riemann)	$\mathrm{Li}(x)-\frac{1}{2}\mathrm{Li}(x^{\frac{1}{2}})$
4		$x\Big/\left(\ln x-1-\frac{1}{\ln x}\right)$
5		$x/(\ln x-1)$

[224] **表 90　0 到 x 之间的素数个数的近似公式**

在 1 到 9000000 之间,黎曼近似公式的那条曲线碰到或穿过 0 偏差线(无偏差的横轴)不少于 19 次.

圆周长与直径之比,即圆周率 π,经常出现在与圆毫无关系的场合.一些概率问题里头不时出现这个常数.有一个概率趣题说,如果有两个人,各自随便写出一个正整数,则这两个数互质的概率是 $6/\pi^2$.若两个人各自随便写出 1000 个数,再算一下这些数之间有多少对是互质的,把此数除以 1000,并令它等于 $6/\pi^2$,由此计算 π 值,据说其正确程度相当可观.也许读者们愿意试做一下这个实验.当然,如果用 10000 次试验代替 1000 次,近似程度会更好一些.

小于给定数 x 的素数个数 N,也可通过一个更为简单但正确度不太高的表达式 $x/\ln x$ 来给出.因此,人们可以粗略地说,一个很大的数目不是素数的机会大体上是 $\ln x$ 与 1 之比.

*　　*　　*

关于素数,存在着许许多多富于挑逗性的猜想,它们看上去像是真的但却无法证明.读者中如能证明它们之中的任何一个,他肯定能在数学的圣贤祠中找到一席之地,同费马与高斯的精

灵在一起干杯!

有关素数的猜想与未解决问题

1. 证明哥德巴赫(Goldbach)猜想:每个偶数都是两个素数之和. 例如:$12=5+7$;$18=7+11$;$100=3+97$.

2. 曾经有人猜想:每个偶数都能用无限多种方式表为两个素数之差. 这是真的吗? 例如:$12=19-7$ 或 $29-17$ 或 $23-11$.

3. 作为上款的特例,偶数 2 是可以这样表达的,因此必定存在着无穷多对素数,其差为 2. 这样的素数称为孪生素数. 例如:在 $n=4$;6;12;18;30;1006428;999999999960;1000000000062;1000000000332;1000000009650;140737488353508;140737488353700 时,$n-1$ 与 $n+1$ 都是素数;另外,当 x 从 1 到 20 时,由公式 $n=30(2x-27)(x-15)$ 给出的 n,也同上面所说的 n 一样,可从它得出孪生素数.

4. 任何偶数可以有无限多种方法表示为两个相继素数之差. 例如:$6=29-23$;$37-31$;$53-47$;$99929-99923$. 还有,$10=23-13$;$41-31$;$71-61$;$99971-99961$.[①]

[225]

5. 具有 x^2+1 形式的素数是否有无限多个? 例如:1^2+1;2^2+1;4^2+1;6^2+1;10^2+1.

6. 是否在相继出现的三角形数或正方形数之间至少存在一个素数? 对 9000000 以下的数目,这是对的.

7. 求出一个大于给定素数的素数,或者求出紧跟在已知素数后面的素数.

8. 给定 n 时,直接计算第 n 个素数.

9. 求出不大于给定数的素数个数.

10. 任何 $4x-1$ 形式的素数是 $4x+1$ 形式的素数及后一形

① 原文如此. 显然作者的说法有漏洞,13 与 23 不是相继素数,其中还有 17 与 19 等等. —— 译者注.

式素数的二倍之和.

11. 在 n^2 与 n^2-n 之间,或者在 n^2 与 n^2+n 之间,至少存在着一个素数.

12. 在大于 3 的两个连续素数的平方之间至少存在着四个素数.

有关素数的经验法则及其例外

1. 哥德巴赫通过观察发现,任何奇数要么是一个素数,要么是一个素数与一个平方数的二倍之和. 例如 $21=19+2$ 或 $13+8$ 或 $3+18$. 据说直到 9000 为止,唯一的例外是 $5777=53\cdot109$ 与 $5993=13\cdot641$,它们既非素数,亦非素数与平方数的二倍之和.

2. 素数可表示为另一素数与平方数二倍之和,但 0^2 不算. 例如 $37=29+8=19+18=5+32$. 直到 9000 为止,例外情况有 17;137;227;977;1187 与 1493,它们作不了以上表示.

3. 1848 年,德·波利纳克(de Polignac)猜想:任何奇数都是素数与 2 的一个乘幂之和,例如 $107=43+2^6=103+2^2$. 他声称已对此性质验证到三百万,后来却又承认 959 不能作以上表示. 本书作者随便挑了几个数:509;977;877,发现这些正整数肯定也属例外情况. 读者们能否发现其他数目呢?这个猜想肯定在什么地方出了毛病.①

4. 至少可以上到 10000,任一偶数都是一个素数与一个乘幂之和;除 1549 外,这一性质对奇数也成立,例如 $856=127+9^3$,$977=761+6^3$.

[226]

* * *

有关素数的下列成果也是令人颇感兴趣的.

① 事实上,现已证明:存在着无限多个奇数不能作以上表示. 请参阅《数学》杂志,34 卷(1960—1961),316 页. ——原注.

有人曾验证到6百万，随后证明了一般情况，即当x大于3时，在x与$2x-2$之间至少存在着一个素数，这就是有名的贝特朗(Bertrand)假设.

1937年，有人证明：一个"充分大"的奇数可以表示为三个素数之和.

* * *

如果$4x+1$形式的正整数能正好用一种方法表示为两个平方数之和，而且，平方数又是互质的话，则这个正整数必定是一个素数或者素数的平方. 如果该正整数并不是很大，或许它是确定其是否为素数的快速而有效的办法.

威尔逊定理不妨在这里再提一下：当且仅当p为素数时，$(p-1)!+1\equiv 0 \bmod p$.

有时也可用费马定理证明一个数为素数. 我们知道，p为素数时$a^{p-1}\equiv 1 \bmod p$. 但对合数模来说，同余式有时也能成立. 模为素数时，可能存在较小的指数使同余式成立(例如，若a不是p的原根时)，但在合数模N的情况下，同余式对一个比$N-1$为小的指数必定成立. 对能使同余式$a^e\equiv 1 \bmod p$成立的小于p的指数e来说，e与$p-1$必有公因子，因此，为了验证对给定值p与a，同余式能否成立，我们只要考虑$p-1$的除数，拿它来试一试就行了. 因而，如果没有一个$N-1$的真除数f能使$a^f\equiv 1 \bmod N$成立(a可选为较方便的很小底数，譬如2或3)，则N必为素数. 而如果$N-1$的真除数的确能满足$a^f\equiv 1 \bmod N$的话，则N可以是素数，也可以是合数. (当然，在寻找$N-1$的因子时有可能和寻找N的因子同样困难.)于是，如果很小的底数(2或3)不属于$N-1$，则表明底数是N的一个原根，从而肯定了N是个素数. 作为一种判定N是否素数的测试办法，费马定理是不能使用的(见第6章). D·H·雷默曾利用本方法的改进形式，在处理极其庞大的数目时取得了辉煌成果.

显然，如果a^{N-1}按模N不同余于1，则N肯定是合数，尽管

它的因子仍属未知.

[227]

* * *

法国数学家E·V·卢卡曾得到一个数列4;14;194;37634;…;$u_n=u_{n-1}^2-2$,其通项公式的构成方法是把一项平方,再减去2,即得下一项.卢卡曾利用这个数列来测试梅桑数的素性.D·H·雷默把卢卡测试法改进为较简便的形式:"当且仅当2^n-1能整除数列的第$(n-1)$项时,2^n-1为素数,否则是合数."例如,2^3-1是14的一个因子,因而$2^3-1=7$是个素数.请读者参阅第3章,那里面介绍了在数字计算机上通过卢卡试验计算大素数的情况.

* * *

存在着无限多个回文素数.下面略举一些:101,131,151,181,313,353,727,757,787,797,919,929,…,79997,91019,93139,93739,94049,…,98389,98689,…,1818181,7878787,7272727,3535353.

* * *

乌思宾斯基与希斯莱特在他们的《初等数论》一书中写道:"在迷人的素数分布问题上,我们只能满足于罗列事实.它们的证明属于解析数论范畴,那是本学科的一个极其广阔而艰难的分支,在那里,数的性质是要用包含超越概念(如连续性)的方法去加以研究的,如此等等."让我们引用他们的话来结束本章.

参考文献

Ball, W. W. R. *Mathematical Recreations and Essays*. New York: Macmillan Co., 1939.

Bell, E. T. *The Last Problem*. New York: Simon and Schuster, 1961.

Crocker, R. "A Theorem Concerning Prime Numbers," *Mathematics*, **34**(1960—1961), 316.

Dickson, L. E. *History of the Theory of Numbers.* 3 vols. New York: Chelsea Publishing Co., 1950.

——. *Introduction to the Theory of Numbers.* New York: Dover Publications, Inc., 1957.

Gillies, D. B. "Computer Discovers New Prime Number," *Science News Letter*, **83**(May 11, 1963), 291.

Glaisher, J. *Factor Tables for the Sixth Million.* London: Taylor and Francis, 1883. [228]

Hardy, G. H. "An Introduction to the Theory of Numbers," *Bulletin of the American Mathematical Society*, **35**(1929), 778.

——, and Wright, E. M. *An Introduction to the Theory of Numbers.* Oxford: Clarendon Press, 1954.

Hurwitz, A. "New Mersenne Primes," *Mathematics of Computation*, **16**(1962), 249.

Lehmer, D. N. *Factor Tables for the First Ten Million.* New York: Hafner Publishing Co., 1956.

Mapes, D. C. "Fast Method of Computing the Number of Primes Less Than a Given Limit," *Mathematics of Computation*, **17**(1963), 179.

Martin, A. "Prime Numbers in Arithmetical Progression," *School Science and Mathematics*, **13**(1913), 793.

Mathews, G. B. *Theory of Numbers.* New York: Chelsea Publishing Co., 1961.

National Bureau of Standards. "National Bureau of Standards Western Automatic Computer," Technical News Bulletin, **37**(Oct., 1953), 145.

Ore, O. *Number Theory and Its History.* New York: McGraw-Hill Book Co., 1948.

Reid, C. "Perfect Numbers," *Scientific American*, **188** (March, 1953), 84.

Starke, E. P. "Palindromes in Progression," *Mathematics*, **29** (1955), 110.

Uspensky, J. V., and Heaslet, M. A. *Elementary Number Theory*. New York: McGraw-Hill Book Co., 1939.

Van Der Pol, B. "Radio Technology and Theory of Numbers," *Journal of the Franklin Institute*, **255**(June, 1953), 476.

——. "An Addendum and Corrections to 'Radio Technology and Theory of Numbers,'" *Journal of the Franklin Institute*, **256**(Sept., 1953), 265.

Vinogradov, I. M. *Elements of Number Theory*. New York: Dover Publications, Inc., 1954.

Wright, W. C. *Wright vs. Eratosthenes*. Boston: G. H. Ellis Co., 1915.

[229]

第21章 分　解

在数论中几乎没有别的课题比分解一数为其素数因子更吸引人了.目前在这方面已有了变化多端、精巧绝伦的方法,但它们犹如毒药浸过的常春藤疗法,没有一个是特效药.某种办法也许只要用3到4步即可分解一个10位数;但对一个6位数,同样的办法也许要花费50步或更多的步数.

新手们听到以下事实时,常会感到吃惊:原来竟然没有一个简单的直接方法来求出一个数的除数.因子分解与除法截然不同.对除法来说,已给出了被除数与除数,而对因子分解来说,已知的只是被除数,又不存在普遍而实用的法则来判定该数除了1与本身之外有无其他除数.

倾听一下外行人的意见或许是相当有趣的:他们是怎样来分解一个数为其因子的?不妨拿数221来作具体例子.一般他们不断地用整数2,3,4,5,6,7,…去试除,人家问他们这种做法要走得多远时,通常的答复总是,一直要试除到原数的一半(对本例来说是111)为止.但实际上,只需要试除素数除数就行了,因为倘若某数有一合数除数,则该除数的素因子必然也能整除该数.进而言之,凡是大于某数平方根的素数也不必进行试除,因若有一个大于平方根的除数存在,则由此而得的商数必然小于平方根.

现在,对221来说,平方根小于15,因此,我们要考虑的素除数,六个即已绰绰有余,它们是2,3,5,7,11与13.前面三个

整数立即可以排除(2 与 5 不会是除数,因为 221 是个奇数,且末位数又不是 5;3 也不可能是除数,因为 221 的各位数码之和不能被 3 整除);7 与 11 都不能整除 221;最后,13 把 221 除尽无余,商数是 17.

较诸平方根制约更少为人知晓的是下列事实:如果某数的最小素除数大于其立方根,则该数只可能再有另一素除数.略为[230]思考一下即能理解何以如此:由于数 N 的最小除数 d 大于 $N^{\frac{1}{3}}$,所以较大除数 D 一定要小于 $N^{\frac{2}{3}}$. 如果 D 有一个真除数的话,则它必然小于 $N^{\frac{2}{3}}$的平方根,亦即 $N^{\frac{1}{3}}$. 但这与已知条件发生抵触,因假设最小除数要大于 $N^{\frac{1}{3}}$. 由此推出 D 不可能有真除数,它必须是个素数.从而可知,N 只有两个素数真除数 d 与 D.

尽管这些制约条件相当可观地削减了试除工作量,但即便把它们用来对付一个四位或五位数,依然是不切实际的.譬如说要测试的数是 33029,正好小于其平方根的最大素数是 181,小于或等于此数,从而需要进行试除的全部素数共有 42 个.经常采用的高效率办法是利用平方数表(巴罗表可以一直上到 100000000)以及第 15 章中讲过的办法,以确定该数究竟能用多少种不同方法表示为两个平方数之和.由于 33029 是一个 $4x+1$ 形式的自然数,如果它只能用一种办法表示为两个平方数之和,而这两个平方数又是互质的话,则该数必定是一个素数或素数的平方;如果两平方数并不互质,则其公共除数必定是原数的一个除数.至于要区别素数或素数的平方,那是很容易的,只要开一下方,看看平方根是不是整数就行了.如果 $4x+1$ 形式的数不能表示为两个平方数之和,则它必定是合数,并包含偶数个 $4x-1$形状的素因子.至于 $4x+1$ 形式的素因子,可能存在,也可能不存在.这两种因子都不能用平方和方法来决定.

如果原数能用不止一种的办法表示为两个平方数之和,这说明该数是一个合数.如果只有一种办法表示为两个互质的平

方和，则原数是单个素数的立方或高次幂；如果两互质平方数的记法不止一种，则原数是至少两个素数的乘积. 如果两个平方数并不互质，则它们的最大公约数是该待定数的一个因子.

第 15 章中所列举出来的平方数的 22 种两位尾数对我们的问题也颇有帮助，它使我们只要去考虑四类从 33029 减去的数就行了，其结尾是 00；04；25；29. 另外，要进行试探的平方数必定位于从 1 到原数一半（即 16384）的范围以内，这样的平方数一共有 36 个. 碰得很巧的是，第一个小于 16384 的平方数 16129，就能使相减后的差数 16900 恰为一平方数，于是我们得到 $33029=130^2+127^2$. 由于再也找不到其他平方数使从 33029 [231] 减去此数后，所余之差数仍为平方数，从而我们得以判定 33029 是一个素数（显然，把 33029 开方，得到的是不尽根）.

当一数能用两种或两种以上办法表示为两个互质的平方数之和时，则此数必为合数，并可通过下列办法分解成因子：若 $N=a^2+b^2=c^2+d^2$，则

$$N=(ac+bd)(ac-bd)/(a+d)(a-d) \text{ 或 } (ac+bd)(ac-bd)/(c+b)(c-b). \quad \text{（公式 1）}$$

这些表达式恒能给出整数值，并将 N 表达为两个整数之乘积. 在第 15 章中我们已求出过 $16000001=4000^2+1^2=1049^2+3860^2$. 从而有 $a=4000, b=1, c=1049, d=3860$. 于是

$$\begin{aligned}16000001 &= (4000\cdot 1049+3860)(4000\cdot 1049-3860)/(1049+1)(1049-1)\\ &= (4199860\cdot 4192140)/(1051\cdot 1048)\\ &= 229\cdot 69869.\end{aligned}$$

容易查明 229 是个素数. 至于 69869 这个数，因它属于 $4x+1$ 形式，我们仍可以进行尝试，把它表示为两个平方数之和. 由于此数以 69 结尾，可见只有以 00，25，44，69 结尾的平方数才能留下

平方数的差数.略试数次我们即可发现 $68644=262^2$ 能留下平方数的差数225,而 $56644=238^2$ 的相应平方数差数是13225,从而可知 $69869=262^2+15^2=238^2+115^2$.同以前一样,利用公式1分解因子,可得 $69869=109\cdot 641$,于是最后得到全部素因子分解式:$16000001=229\cdot 109\cdot 641$.

此法不仅限于待分解数可表示为平方和,当它能表示为 x^2+ky^2 形式时亦可使用.我们有下述公式:

$$(x^2+ky^2)(m^2+kn^2)=(xm+kyn)^2+k(xn-ym)^2$$
$$=(xm-kyn)^2+k(xn+ym)^2,$$

此式表明:如果乘积的形式是一平方数加上另一平方数的 k 倍,则它的每个因子也必具有此种形式.例如,$(2^2+5\cdot 3^2)(3^2+5\cdot 4^2)=66^2+5\cdot 1^2=54^2+5\cdot 17^2$.

把上式过程逆转,若 $N=a^2+kb^2=c^2+kd^2$,则

$$N=k(ad+bc)(ad-bc)/(a+c)(a-c),\text{或}$$
$$(ad+bc)(ad-bc)/(d+b)(d-b),\quad(\text{公式 }2)$$

同前面的结果也很类似.

[232]

* * *

分解因子时通常使用"排除元"方法,它是很有效的.它可以迅速判定,一数能表示为二次形式 x^2+ky^2 的方法种数.在此之后,即可用上述办法分解因子.

在 x^2+ky^2 中,$k=4,2,-2$ 时相应的二次形式 x^2+4y^2,x^2+2y^2,x^2-2y^2 可用以表示一切奇整数.例如,第一个形式可表示 $8x+1$ 或 $8x+5$ 形式的整数;第二个形式表示 $8x+1$ 或 $8x+3$ 形式的整数;而最后一个形式表示 $8x+1$ 或 $8x+7$ 形式的整数.若待分解数为45677,由于它属于 $8x+5$ 形式,所以我们决定采用二次形式 x^2+4y^2.于是 $y=[(45677-x^2)/4]^{\frac{1}{2}}$,$y$ 必须小于107.为了避免试探一切 x 值的冗长与单调,可以使用类似

第19章中说过的一种排除法.

我们要去解不定方程 $45677-4y^2=x^2$. 取一个较小的模数5作为排除元,即可得到 $2-4y^2\equiv x^2 \bmod 5$,因此只需考虑能使 $2-4y^2$ 得出5的一个平方剩余(1或4)的那些 y 值就行了. 这样一来,形式为 $5z$, $5z+1$ 或 $5z+4$ 的那些 y 值就统统被排除,因为在那种情况下, $2-4y^2$ 的对应余数将是2,3,3,而它们都是5的平方非剩余. 需要保留的形式是 $5z+2$ 与 $5z+3$,它们将能使 $2-4y^2$ 分别同余于1或4. 继续采取同样的步骤,不断使用排除元7,8,9,11(素数或素数的乘数),剩下来的就只有7,17,23,27,53,67,77这几个数,试探的工作量便从107个一下子削减为7个. 稍经试探,便可看出,数17能给出 $45677-4\cdot 17^2=211^2$,而 y 的任何其他值都产生不出平方数的剩余,从而可以判定45677乃是一个素数.

再试一次,设给定数 N 为36661,它属于 $8x+5$ 形式. 于是可以寻求不定方程 $x^2+4y^2=36661$ 的解,由排除元方法得以找出关系式 $36661=169^2+4\cdot 45^2=119^2+4\cdot 75^2$. 此处 $a=169$, $b=45$, $c=119$, $d=75$,利用公式2,即有

$$N=(169\cdot 75+45\cdot 119)(169\cdot 75-45\cdot 119)/288\cdot 50$$
$$=61\cdot 601,$$

故36661是这两个素数因子61与601的乘积.

已经编造了用于同余关系的排除元表,以便迅速地除去不合要求的那些 y 的形式,为了找出其后所需要的形式,也造出了一些镂空模板.

或许读者们想尝试一下,自己是否已经掌握了这种方法,那就请试试,把以下各数分解因子:(a)23449;(b)394831;(c)16503593;(d)18000001. †

[233]

* * *

利用平方剩余也许是大数分解因子的一种最有效的办法.

第 19 章与第 22 章解释了怎样获取一个数的较小平方剩余的方法. 基于此种信息的因子分解法立足于以下事实:若 R 是待分解数 D 的一个平方剩余,则它必然也是 D 的任一素因子的平方剩余. 于是人们得以计算并用列表形式给出以给定数 R 为平方剩余的一切素数(在某个实用上限以下). 如果已经有一些 D 的平方剩余被求了出来,人们就可以查看每个平方剩余所对应的素数(为了方便起见,要将每个平方剩余做成一张卡片),再看看究竟有哪些素数是已知一切平方剩余所公有的,它们就是 D 所具有的、唯一可能的素数除数. 如果有一打左右较小的平方剩余是已知的话,那就会大大限制了一个九位或十位数所可能具有的素因子的个数. 如果没有一个素数为已知平方剩余所公有,这就表明 D 本身是一个素数.

在平方剩余卡片上检索哪些素数是公有的,一个干脆而利索的办法是在卡片的指定位置上打洞或穿孔. 于是,叠合在一起的平方剩余卡片(有时称为因子模板),就能使光线通过洞孔,表明处在这个位置上的素数是 D 的可能素因子. 如果任一洞眼都不能透过光线,则意味着 D 本身是个素数. (模板上记录的素数至少应包含 D 的平方根所限定的素数在内.)

图 21 是商用机器上处理数据用的标准霍尔瑞斯卡片[1]的一张复制品. 卡片上一共有 800 个单元(或孔位),每个单元都对应于一个素数. 图示的卡片在一些素数单元处穿孔,这些素数全都具有 29 作为其平方剩余. 按照自然顺序,第 800 号素数为 6131,它是 37589161 的平方根. 因此,每张具有 800 个单元的一套模板已经足够用于将近四千万个数目的因子分解.

正、负平方剩余都不超过 250,且不包含平方因子的各个因子模板都已经编造成功. 标准尺寸的霍尔瑞斯卡片略显容量不

[1] 赫尔曼·霍尔瑞斯(Herman Hollerith),1860—1929,美国发明家,他曾利用凿孔方式把各种文字与数据信息在卡片上编码,用途甚广. ——译者注.

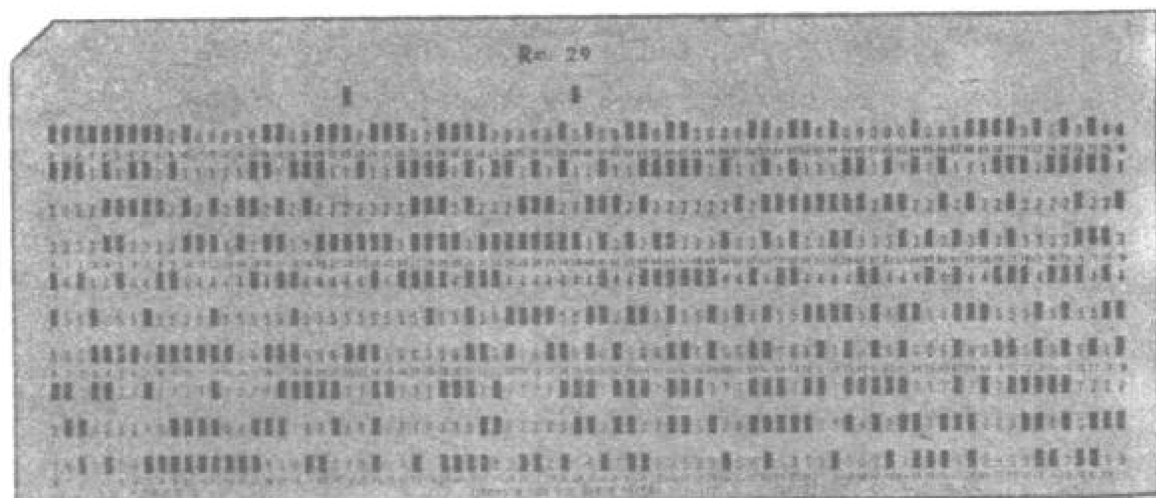


图 21 一块因子模板

〔234〕

足，这个缺点也已克服. 人们使用了七种颜色来表示一个剩余，这样一来，就给出了 5600 个单元，也就是 5600 个素数. 第 5600 号素数是 55079，其平方数为 3033696241，模板演进到这一阶段，在此范围内的自然数即可快速地分解因子. 如果已知某数的最小素因子不超过 55079，则其适用范围尚可大大超越.

承蒙密执安州大学埃尔德(J. D. Elder)博士的好意，笔者手里终于有了一套较小的模板，足以对 37589161 以下的自然数进行因子分解，它们的使用给笔者带来了很大乐趣.

*　　　*　　　*

上述方法十分精致而有效. 另外的办法可能容易掌握一些，但一般说来用途有限，因为除了最有利的情况之外，所需的工作量大得惊人. 费马曾经用过下列办法：设 N 是待分解数，r^2 是刚刚大于它的最小平方数，令 $N=r^2-A_0$. 如果 A_0 是一平方数，则 N 已被表示为两个平方数之差，从而即可分解因子. 如果 A_0 不是平方数，则我们还可以有一系列等式：

$$
\begin{aligned}
N = r^2 - A_0 &= (r+1)^2 - (A_0 + 2r + 1) \\
&= (r+2)^2 - (A_0 + 2r + 1 + 2r + 3) \\
&= (r+3)^2 - (A_0 + 2r + 1 + 2r + 3 + 2r + 5)
\end{aligned}
$$

$$\cdots\cdots$$
$$= (r+n)^2 - A^2 = (r+n+A)(r+n-A).$$

换言之，我们在 A_0 之上再加 $2r+1$；若结果得出一个平方数，我们就已将 N 表示为两个平方数之差；若结果不是平方数，则再加 $2r+3$，$2r+5$，$2r+7$，等等，直到得出平方数 A^2 为止，于是就有 $N=(r+n+A)(r+n-A)$.

设 $N=340663$. 于是 $r^2=344569=587^2$ 是刚超过 340663 的最小平方数，但此时的差数 $A_0=3906$ 不是平方数. 在 3906 之上加 $2r+1=1175$，结果5081仍不是平方数. 于是在5081上再加 1177，所得的结果 6258 还是不行. 这样，我们不断加上 1179；1181；1183；最后得到 9801 是 99 的平方，这是仅仅经过五次递加而得到的结果. 于是

[235]

$$340663 = (587+5+99)(587+5-99) = 691 \cdot 493.$$

第二个因子 493 为一合数，它等于 $17 \cdot 29$，所以最后结果为 $340663=17 \cdot 29 \cdot 691$. 通过这种办法，费马只用了 11 次加法，就把一个十位数分解出因子：

$$2027651281 = 44021 \cdot 46061.$$

而用通常的试探法，在 44021 以下的奇素数，共须进行 4580 次除法，工作量之差别何等悬殊！但这可能是一个特别有利的场合，存心被用来夸耀本法力量的. 实际上，比上述小得很多的数字，所需的工作量也许大得不切实际.

还有一个相当粗糙的办法，有时也能快速奏效. 其办法是在 N 之上不断添加 $1^2, 2^2, 3^2, \cdots, x^2$，直到结果 y^2 是一平方数，于是有 $N+x^2=y^2$，而 $N=(y+x)(y-x)$. 要添加的平方数个数可利用平方数的两位或多位尾数来进行削减与控制. 例如待分解数是 10541. 平方数表告诉我们，下一个较大的平方数为 $10609=103^2$，但由于差数的末位数是 8 而显然不行. 下一个平

方数 $10816=104^2$ 将给出差数 75，它仍不是平方数．然而再下一个 $11025=105^2$ 将给出差数 484，后者正是 22 的平方．于是 $10541+22^2=105^2$，而

$$10541=105^2-22^2=(105+22)(105-22)=127\cdot 83.$$

再试一下，取 $N=119143$，大于此数的平方数只要试七次，即可发现 $119143=123904-4761=352^2-69^2=(352+69)(352-69)=421\cdot 283$，后面两个因子都是素数．

由于大于 1 的任何奇数总可以表示为两个平方数之差，所以我们在一个性质未定的奇数上加上平方数，最终必然会得出一个平方数的．但若待定性的数碰巧是个素数，那就会花费很多步数才能得出平方数．所以在经过多次尝试后仍然得不出预期结果的话，那么最好放弃这种办法．例如，对一个很小的数 9839 来说，人们几乎要查阅巴罗表中一半的平方数，然后才能发现 $9839+4919^2=4920^2$，于是才能得出 $9839=(4920+4919)(4920-4919)=9839\cdot 1$，最后表明 9839 是一个素数． [236]

另一种时常奏效的分解办法是余数法．设 N 是待分解数．求出不超过 $(N-1)/2$ 的最大平方数 a^2，并令 $(N-1)/2-a^2=r$．将 $a\cdot a$ 放在第一纵列，$2r+1$ 放在第二纵列．然后在第一纵列里不断写下 $(a+1)(a-1)$，$(a+2)(a-2)$，等等；在第二纵列里写下 $2r+3$，$2r+9$，$2r+19$，$2r+33$ 等等，即第一次把该列首数加 2，以后每次加数都得再递增 4．换言之，要不断加上 2，6，10，14，18，…以得到该列中的下一数．接着需要察看，第一列中的各数与第二列中的对应数之间有没有公因子，如果有的话，则此公因子也必然能整除 N．

例如设 $N=142397$，则 $(N-1)/2=71189$．不超过此数的最大平方数是 $70756=266^2$，于是有 $a=266$，$r=71198-70756=442$．照上法造出两个纵列来：

n	$(a+n)\cdot(a-n)$	$(2r+1)+2n^2$	差数
0	266 · 266	885	
1	267 · 265	887	2
2	268 · 264	893	6
3	269 · 263	903	10
4	270 · 262	917	14

于是发现 131 能整除 262 与 917，从而也能整除 142397，而其商数是 1087.

这个方法也可以用代数形式描述如下：由于$(N-1)/2=a^2+r$，故有

$$
\begin{aligned}
N &= 2a^2+2r+1\\
&=2(a+1)(a-1)+(2r+1+2)\\
&=2(a+2)(a-2)+(2r+1+2+6)\\
&=2(a+3)(a-3)+(2r+1+2+6+10)\\
&\cdots\cdots\\
&=2(a+n)(a-n)+[2r+1+2+6+10+\cdots+(4n-2)]\\
&=2(a+n)(a-n)+[(2r+1)+2n^2]=N.
\end{aligned}
$$

如果能找到一个数，可同时整除方括弧内的表达式以及$(a+n)$或$(a-n)$中的一个，则此数必然能整除 N. [237]

让我们通过这种办法来分解数 16000001. 此处$(N-1)/2=8000000$，不超过此数的最大平方数 a^2 是 $2828^2=7997584$. 于是 $r=8000000-7997584=2416$，而所谓的两个纵列将是：

n	$(a+n)\cdot(a-n)$	$(2r+1)+2n^2$	差数
0	2828 · 2828	4833	
1	2829 · 2827	4835	2
2	2830 · 2826	4841	6
3	2831 · 2825	4851	10
4	2832 · 2824	4865	14
5	2833 · 2823	4883	18
6	2834 · 2822	4905	22

此时可以发现 2834 与 4905 有一最大公约数 109，从而判

定 109 是 16000001 的一个除数.最大公约数的求法是：从一数的若干倍数中减去另一数的倍数，使所得的差数容易分解成素因子，并可由此判定这些素因子能否整除原来的两数.其细节可以参阅几乎任一本代数教科书.对本例来说 $4905=5\cdot 981=5\cdot 9\cdot 109$，由于 109 能整除 2834，然而 5 与 9 不行，故可判定 109 是 2834 与 4905 的最大公约数.于是，仅仅经过七次试探，我们就分解出了一个很大数 16000001 的因子.

即便对于小得多的数字，这个方法也不见得总是走好运的，此点可通过数 7031 来说明.这里，$(N-1)/2=3515$，$a^2=59^2=3481$，$r=3515-3481=34$.

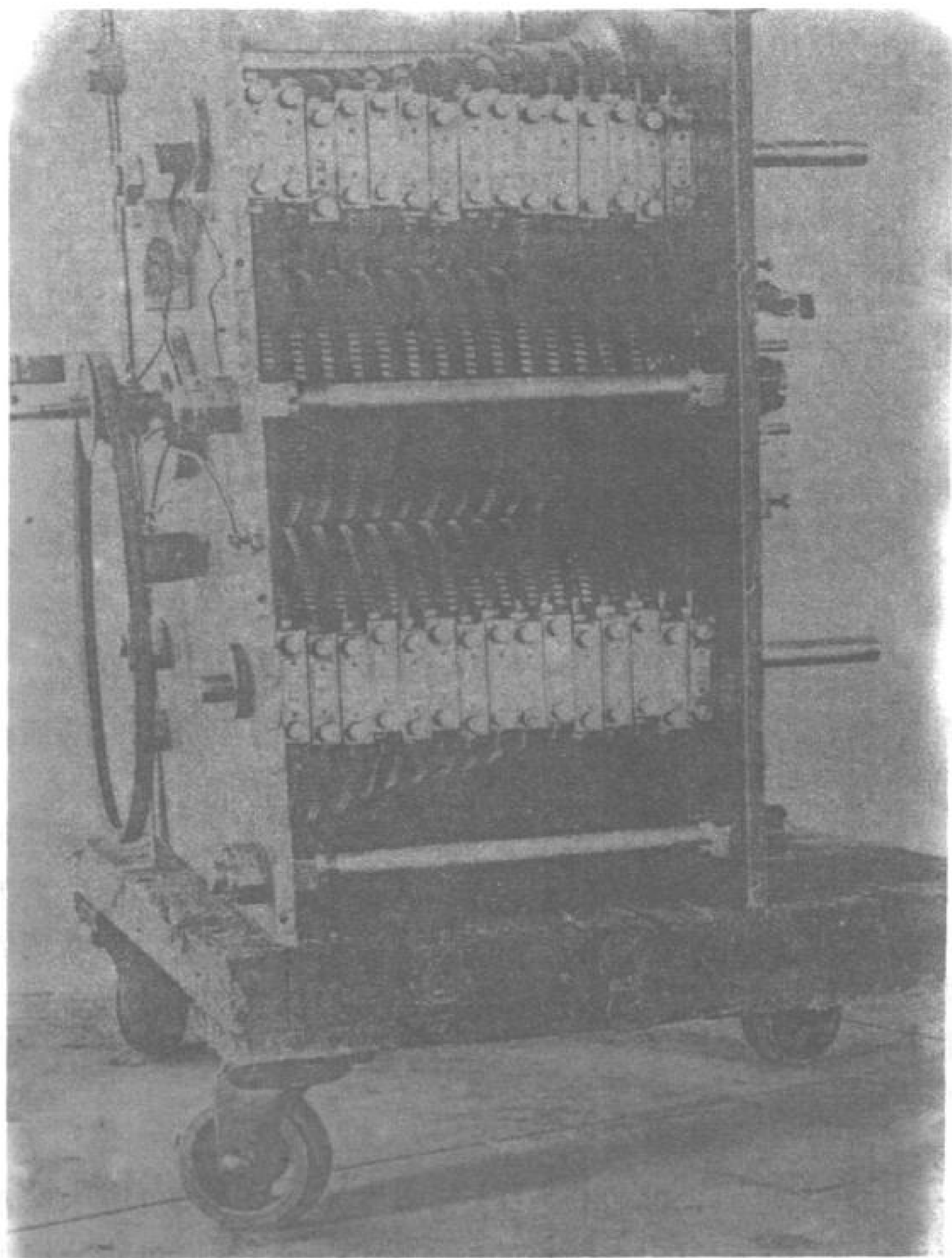
n	$(a+n)(a-n)$	$(2r+1)+2n^2$
0	$59\cdot 59$	69
1	$60\cdot 58$	71
2	$61\cdot 57$	77
…	…	…
20	$79\cdot 39$	869

需要经过 20 次试探才能肯定 79 与 869 具有公因子 79，从而得知 $7031=79\cdot 89$.

但是，如果改用添加平方数的办法，只要经过一次试探即可得知大于 7031 的平方数是 7056，而差数 25 又正好是个平方数，于是有 $7031=84^2-5^2=(84+5)(84-5)=89\cdot 79$.此例表明，对任何一种分解办法都不应过分热心；世人还是要等待另一个费马或高斯的降生，以发现一种普遍而有效的办法，可以一下子直插任何因式分解问题的核心. [238]

* * *

加利福尼亚大学的 D·H·雷默博士及其父亲 D·N·雷默博士发明了一台引人注目的因子分解机器，从而可使分解大数时所需的庞大工作量得以大大削减.由于它的问世，终于完成了势将花费若干位手工计算者终身劳动的某些大数的因子分解.



[240] 图版 A 雷默博士的因子分解机器

$2^{93}+1$ 有一个庞大的、未征服因子

$$1537228672093301419=(2^{62}-2^{31}+1)/3,$$

在把它提交给机器之后三秒钟，机器就停止运转，有迹象表明，猎物已经在望. 简短的计算给出了两个因子 529510939 与 2903110321. 由于 $2^{93}+1=(2^{31})^3+1=(2^{31}+1)(2^{62}-2^{31}+1)$，于是 $2^{93}+1$ 的素因子都已查明，完成了全部分解过程，因为以前的计算者已经发现 $2^{31}+1=3\cdot 715827883$.

这台机器里有着一套 15 个相同的齿轮，每个齿轮有 100 个牙齿，牢固地安装在公共的中央传动轴上. 在直径对蹠点处相互啮合的是两组传动齿轮，其中每个成员都有着为数不同的、素数个数的牙齿，并独立地围绕着各个不同的中心旋转. 所以，共有 30 个传动齿轮，以对应于从 3 到 127 的 30 个奇素数. 在每个齿轮里都有一个与其旋转中心同心的圆，圆上钻了许多小孔，其个数等于齿数(见图 22). 设想用一根长针(或栓子)穿过每个齿轮的一个洞孔，以便使传动齿轮调节到 0 或初始位置. 则由于各齿轮的洞孔数是互质的，所以决不可能再有别的洞眼位于一直线上. 这时若把长针拿掉，就可以让排成一直线的洞眼穿过一束光线，但当各齿轮用不同速度转动时，排成的一直线当即消失，以后即使再经过成千上万次的齿轮转动，也不能恢复到初始位置. 有时，某些孔眼需要塞住，以免万一发生排成一直线的情况.

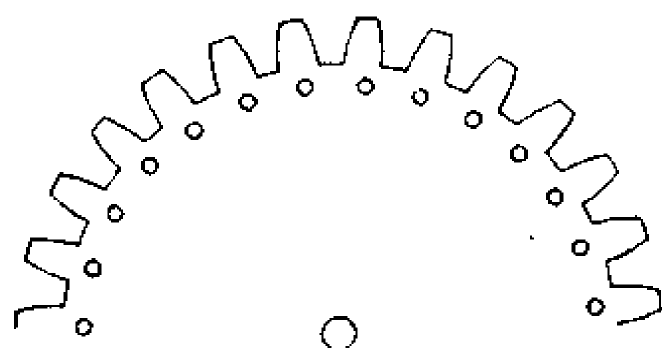


图 22 因子分解机的齿轮

通过一系列传动齿轮的光线经过两个棱镜的反射之后进入[239]第二组齿轮，撞击在一个光电池上．在适当放大以后，光束所产生的电流足以使传动系统停下来．当洞眼排成一直线时（意味着有一个解），光线就会在万分之一秒内落在灵敏的光电"眼"上，经过 729000000 倍的放大，使继电器获得充分能量使机器停止．然后，通过转速记录表就可以知道机器的转动情况，再经过简单计算，就找到了因子．

通过以上描述，可以领会到因子分解机原来是把一个数迅速同时表达为许多不同形状的快速装置，从而可以在合理的时间限制内把给定数的可能除数加以限制．

建造这台机器所遇到的困难，怎样排除障碍与最终使之正常运行，这些事情读起来真像一部冒险故事．光线是如此微弱的一个脉冲信号，它要与光电池"交谈"的时间又是如此短促，这都要求机器的任何一个局部都必须制造得高度精确，而且还必须调整得无懈可击，能量放大高达 729000000 倍，这也是个骇人听闻的数字，放大器既然如此灵敏，哪怕任何一点点震动摇晃，电流的一个微小变化，电器的开或关，甚至在场者的一句鲁莽说话都有可能导致机器的喜怒无常，从而使表演失败．

发明家的父亲，已故的 D·N·雷默博士，他既是一位数学家，又是一位诗人，曾经栩栩如生地描写了这台机器降生时的分娩阵痛以及其后的出色表演[1]：

> 放大器被安放在另外一间房子里，用一堵厚厚的[241]砖墙把它同快速旋转的齿轮组隔开，并密封在一具隔音板做的木头棺材里．这种做法使机器的运行情况变得稍好一些，但它仍为一种完全无法预测的颤动起伏

---

[1] 请参阅：D·N·雷默博士所写的"机器进行困难的数学计算"一文，原载《新闻服务公报》，第 3 卷第 3 期，华盛顿卡内基学院，1939 年．——原注．

所左右。机器在愉快而美妙地运转几分钟后突然变得无头无脑。一会儿又拉扯在一起，以完全理性的方式正常运作了刻把钟，然后，坏脾气又发作起来。而这一切，几乎都是在周围环境看不出有一点点变化的情况下发生的。

“医生”们被请来了，但从这些症状中推断不出机器究竟生了什么“病”。在放大率高达七亿倍以上的条件下要求机器能稳定地正常工作，这当然绝非易事。好有一比，就像是用一支长达一万英里的大笔而想写出一手轻松流利的书法，何况随时都有一个调皮捣蛋的小鬼在你手腕上跳来跳去。那么，小鬼究竟是什么东西？我们怎样才能把他抓住？

搜捕“小鬼”

日复一日地进行着徒劳无功的调试与再调试，看来并不存在什么器质性的病变，而只是神经质的。然而，这是一个很有趣、很重要的病例，年轻的主管医生不愿意放下病人不管。最后，他忽然想起了使用“听诊器”的办法，于是，他安装了一个扩音器并注意倾听。果然，“小鬼”的藏身之地被发觉了。原来，那是近邻的一个无线电站里正在运转的短波无线电扇风装置的作祟。只要它安静下来不工作，一切就都正常；而它一旦上马，放大器便会痉挛抽搐，电眼也发了红。

没有必要去尝尝它的利害，机器是由于无线电的原因而喜怒无常，对此，人们几乎无计可施，只好把放大器更妥善地进行屏蔽起来，以排除这种有趣而不需要的干扰，或者干脆等待一个无线电操作人员不上班的时间。人们当然也有点思想准备，同余式机器会给他带来许多麻烦事，无论如何，在那台敌对机器得到安

置，短暂的“停战”终于来临之前，实在无事可作.只好等到以太波安静下来，才能把重要的算术问题提交给机器去解决.

攻打数字巨人

那一天是10月9日，正好在发现“小鬼”之后，因子分解机准备启动，去做一做实际的数论研究工作了.选定的那一天是毗邻无线电工作人员不值勤的日子，提交给机器的问题是要找出 $2^{93}+1$ 的一个庞大的，未被人们征服的因子1537228672093301419，此数已由一项强有力的测试，判定其为合数.

用通常办法将此数分解因子，即使最有本事的计算专家也需要终生不懈工作.但是，仅三秒钟左右，在快速旋转的齿轮旁边的“电眼”发出了信号，于是机器突然停了下来.人们起先感到，“小鬼”可能又来捣蛋了.但是，检查察看之后，终于发现那个19位的庞然大物已被分解为两个素数因子：529510939与2903110321.

[242]

这是10月9日中午前后的事.远在伯克利的我，邮件一到便得知信息，当下即把其他事情安排一下，立即启程前往派萨旦那（因子分解机的制造地点）了解情况.我在10月17日傍晚到达，发现一个小团体已准备粉墨登场.贝尔教授，伍尔夫教授，瓦德教授都已被我儿子请来，观看因子分解机能不能攻下历史上的庞然大物，$2^{95}+1$ 的不可征服的因子3011347479614249131，而 $2^{95}+1$ 这个符号所代表的数等于39614081257132168796771975169.

我儿子已掌握了一些必要但尚不够充分的证据，表明此数乃是一个素数.为了确证，他必须先研究较此

数小1的数.而后者可析出较小的因子2,3,5,19.除此以外还有一个因子是5283065753709209,它已被证明为合数,但不知道它的因子究竟是什么.

在攻打这个庞然大物之前,我儿子决定利用一个结果,他已知道此数可表示为一个平方数与另一平方数的七倍之和,如果他再能找到另一个这类表达式,那么他就可以直接分解出因子来.

这个任务交给了机器,要求它找到另一种办法,把这个数字巨人表示为一个平方数与另一平方数的七倍之和.他已把与此问题有关的齿轮上的洞眼作了调整安排,一切都已准备就绪,耐心等待着一个平静时刻的到来以便开动机器.

向吉凶未卜的前境跨出一步

小集团人员紧张万分地注视着机器,它已作好了准备,以考验它能否经受得住外力干扰.零点永远是一个解答,于是他把机器向后倒转运作五分钟,再使它向前转动,看看它会不会错过零点.机器不负众望,很快地跨越了陷阱,看来一切都很顺利."现在我们要向未知境界跨出一步了,"我的儿子说,一面开动了机器.

我在地板上走来走去,极度焦躁不安.机器会不会反复无常呢?无线电"小鬼"会不会再来掣肘捣蛋呢?它有10000000万数据要申报进去,机器开始转动了,时间一分钟、一分钟地过去,我简直有点不敢相信,机器的"眼睛"真的能做到分分秒秒都不放松警惕吗?

在平稳地运转了15分钟之后,隆隆声突然停了下来,我们屏息敛神地看了读数,把结果递交给伍尔夫教授,他是一位计算专家,想了解是否真正找到了正确答数.几分钟后,我们确信果然如此,然后又安排机器来

寻找其他解答.

这一次,隆隆声持续了 25 分钟之后才停下来. 另一个正确答数果然出现了. 几分钟以后,我们终于掌握了两个因子:59957 与 88114244437. 前者易知为素数,后者则尚待确定,下一天,我同我儿子终于解决了它,确证它也是一个素数.

如果你能现场目睹小团体里各位教授及其夫人的激动心情,这定将使你万分惊讶. 我们聚集在实验室里一张桌子的周围喝咖啡,谈论这台机器的神秘与不可思议的威力. 大家都一致同意,凡是能用因子表或镂空模板即可解决的一些小问题是不必劳动这台专用机的"大驾"的. 它是专门用来对付普通望远镜力所不及的、远在河外星系中的庞然大物的. 可以这样说,迄今为止,还没有任何别的装置能与之匹敌.①

来自华盛顿卡内基学院《新闻服务公报》第 3 卷第 3 期的这段有趣报道继续说道:

由德律克・亨利・雷默这位发明家在加利福尼亚州派萨旦那县罗伯特・布德公司实验室建造的这台机器,是把光电池魔术与大数研究巧妙结合的一个首创范例.

人们认为,首先它可用来澄清具有 2^n+1 与 10^n+1 形式的数的因式分解问题,长期以来它们老是挫败了数学家们的不断努力.

除此之外,还有一些问题特别适合于本机器求解. 其中之一便是 18 世纪瑞士数学家李奥纳德・欧拉所

① 现代数字计算机的性能远远超过了这台机器. ——原注.

提出的一个公式及其推广.

欧拉认为,对一切 n 值,表达式 n^2-n+41 恒能得出素数. 尽管此公式对40以下(也包括40本身)的一切 n 值确能得出素数,充分表明公式的素数含量十分丰富. 然而,$n=41$ 时,由公式给出的数1681却是个合数.

利用同余式机器,验证该公式的一系列数据就变得大为方便. 此外还有一些数论领域中的专家们所提出的、经受得住时间考验的著名公式也可以利用该机器进行校验.

[244]

走向未知数字王国,搜寻除数的这份激动心情,在雷默博士为《数学猎奇》杂志第1卷第3期(1933年出版)所写的一篇文章"数论中的一次大猎捕"中也作了绘影绘声的报道. 读过这篇文章的人都被他的热情所感染. 他在那里屏住呼吸地谈到了 $10^{20}+1$ 的一个因子 9999000099990001 终于抵挡不住他儿子的由脚踏车链条齿轮装置演变而成的那台神奇机器的攻击而倒了下来. 他们蹑手蹑脚,小心翼翼地在他们的猎物前面左看右看了将近两个小时. 其中也包括了打开某些平行电路的机械电气接点的合箭——然后,一下子成功了,所有的触点同时断开,机器突然停了下来. 大猎捕行动落下了帷幕,因子也查出来了,它们是1676321与5964848081.

在谈到当时最大的已知素数

$$2^{127}-1=170141183460469231731687303715884105727$$

时,雷默博士说道:"要想到达这颗遥远的星宿,人们将必须用去漫长的、一光年的年数,走完以光年的光年来计算的距离."

通过费马定理的拓广,雷默父子发现了一些奇妙的方法来对付远远超过天文类比的庞然大数. 设 N 是一个性质未定的

数、如对某个底数 b，N 能整除 $b^{N-1}-1$，但与 $b^{(N-1)/p}-1$ 互质（p 是 $N-1$ 的一个素数除数），则 N 的一切素因子都将具有 $px+1$ 形式. 让我们把它叫做定理 A.

例如要把 $2^{73}+1$ 分解因子，已知它有两个因子 3 与 1753，尚待确定性质的是商数

$$N=(2^{73}+1)/3\cdot 1753=1795918038741070627.$$

已知对任选的底数 $b=3$，$3^{N-1}-1$ 能被 N 整除. 另外又已知晓 $N-1$ 有个除数 811，而且 $3^{(N-1)/811}-1$ 与 N 互质. 于是 N 的一

$$52830657537909209 = 59957 \cdot 88114244437.$$

现成的因子分解表指出前者是个素数，而后一个数字 p，通过定理 A 的应用以及 $M-1$ 的素因子 2489947，亦可判定它是个素数.

对底数 3 而言，已知 $3^{N-1}-1$ 能被 N 整除，但 $3^{(N-1)/p}-1$ 则与 N 互质，因而 N 的一切可能除数都应具有 $88114244437x+1$ 的形式. 机器很轻易地处理了为数非常有限的各种可能性，查明 N 确实是一个素数，于是 $2^{95}+1$ 最终得以完成了全部因式分解：

$$3 \cdot 11 \cdot 2281 \cdot 174763 \cdot 3011347479614249131.$$

类似地又对数

$$N = (2^{85}-1)/(2^{17}-1)(2^5-1) = 9520972806333758431$$

进行了测试. 人们发现 $N-1$ 能被 257 整除，而底数 3 能满足定理 A 的条件. 机器终于证明 N 确是一个素数，于是有

$$2^{85}-1 = 31 \cdot 131071 \cdot N.$$

读者们也许会感到奇怪，作为 $N-1$ 的除数，为何上述的 257 能如此轻易地得出. 这是由于应用了一个巧妙的定理所致：

若 p，q 为素数，则

$$[(a^{pq}-1)(a-1)/(a^p-1)(a^q-1)]-1$$

能被除不尽 a^q-1 的 $a^{p-1}-1$ 的任一素因子所整除. 例如，在 $N=(2^{85}-1)/(2^{17}-1)(2^5-1)$中，$p=17$，$q=5$，而 $2^{16}-1$ 具有除数 2^8+1 与 2^8-1. 前者便是素数 257，它不能被 2^5-1 整除. [246] 因而 $N-1$ 能被 257 整除.

于是，通过齿轮的摩擦过程，以前只知道一个孤立因子 2687 的梅桑数 $2^{79}-1$ 终于被彻底征服，一颗外加上去的星号将放在雷默的姓氏旁边，此人的雕像要放在壁龛里供奉着，他的声

名将永垂不朽了.

参考文献

Barlow, P. *Tables of Squares, Cubes, etc.* Chicago: Charles T. Powner Co., 1948.

——. *Theory of Numbers.* London: J. Johnson & Co., 1811.

Carnegie Institution of Washington. "Machine Performs Difficult Mathematical Calculations," News Service Bulletin, **Ⅲ**,3(1933),19.

Dickson, L. E. *History of the Theory of Numbers.* 3 vols. New York: Chelsea Publishing Co., 1950.

Lehmer, D. N. *Factor Stencils.* Washington, D.C.: Carnegie Institution of Washington, 1939.

——. "A Photo-Electric Number Sieve," *American Mathematical Monthly*, **40**(1933),401.

——. "Some New Factorizations of $2^n \pm 1$," *Bulletin of the American Mathematical Society*, **39**(1933),105.

——. "Hunting Big Game in the Theory of Numbers," *Scripta Mathematica*, 1(1933),229.

Uspensky, J. V., and Heaslet, M. A. *Elementary Number Theory.* New York: McGraw-Hill Book Co., 1939.

[247]

第22章 佩尔方程

公元 1066 年 10 月 14 日，“国王哈罗德(Harold)的士卒们像往常一样站得笔直，组成了 61 个方队，每队的人数完全一样．勇士们诅咒那帮厚颜无耻的诺曼人，胆敢闯入他们的国度；萨克森战士们只要挥动战斧，轻轻一击，就会折断他们的长矛，刺破他们的铠甲……哈罗德一跃而起，加入了冲突的行列，萨克逊人队形一变，组成了一个很大的方阵．但闻杀声震天，‘冲啊！’‘杀啊！’‘该死的！’”

据史书记载，倒霉的萨克逊人组成了 61 个方队，每队人数相同，国王哈罗德加入他们的队伍之后，又重新组成了一个庞大的实心方阵．如果用毫无幻想但正确的数学语言，我们得到了一个方程 $61x^2+1=y^2$ 或 $y^2-61x^2=1$.

读者们能不能求出这一大帮萨克逊战士的人数 y^2 呢？†

方程 $x^2-Dy^2=1$ 称为“佩尔方程”．然而佩尔既不是第一个研究它的人，也不是第一个解决它的人！费马，那个给后人制造麻烦的大教唆者，提出了这个方程，向海峡对岸的英国数学家提出了挑战，在他那个时代，这种姿态是司空见惯的．费马的同胞弗兰尼格对 D 的一切允许值一直算到 150，求出了方程 $x^2-Dy^2=1$ 的最小解．他要求英国数学家瓦理斯(Wallis)继续把它算到 200，或者至少要解出两个方程 $x^2-151y^2=1$ 与 $x^2-313y^2=1$，并暗示说，后一方程也许是瓦理斯力有未逮的．可是瓦理斯的朋友勃朗克(Brouncker)勋爵回答说，他只用了一、二

个小时就找到了关系式$126862368^2-313(7170685)^2=-1$，因而

$$x=2\cdot 7170685\cdot 126862368$$

就是方程$x^2-313y^2=+1$的解. 瓦理斯也解出了另一问题，并得出结果

[248]

$$1728148040^2-151(140634693)^2=1.$$

数学家欧拉错误地把勃朗克解方程的方法归到了佩尔名下，尽管历史已经改正了这个错误，然而方程至今仍然称为佩尔方程而不叫费马方程. 佩尔同本问题的关系其实非常疏远，他不过是修改了某人所翻译的、另外人所著的代数书而已——该作者第一个发表了瓦理斯与勃朗克对费马问题的解. 荣誉总是驻足在这种基础上的.

历史纪录表明，早在耶稣基督时代开始前400多年，该问题即已引起公众的注意. 据认为是阿基米德(Archimedes)研究了著名的牛的问题，并为此花去大量愉快而无用的时间. 尽管在执行计算时显示出惊人的技巧，然而仍未能完全算出答案；将来也不大可能算得出来.

阿基米德牛的问题

朋友，请准确无误地算一算太阳底下的牛数，要身心全部投入，如果你自认为还有几分聪明的话. 多少头牛在西西里岛特立那西亚(西西里本岛)平原上吃草？它们按其毛色分成四群：一群奶白，一群乌黑，一群棕黄，一群斑斓. 在每一群里头，公牛都占多数，其中的关系如下：……(接着叙述了第一批的七个条件.)

朋友，如果你能确切告诉我，每群里头的公牛和母牛数，那你就不愧是一位精明计数者，但是你还算不上

一个智慧之士，除非你还能答出附加的问题.（接着又叙述了第8与第9个条件.）如果你能把各群牛的总数统统算出来，那么，我的朋友，你就可以像征服者那样昂首前进，心安理得地在数的科学里稳执牛耳.①

剥掉花言巧语，问题的数学实质是要求出 W,X,Y,Z（分别表示白，黑，斑，黄的公牛数）以及 w,x,y,z（对应的母牛数）等几个数，它们应满足下列条件：

(1)$W=\frac{5}{6}X+Z$，　　(2)$X=\frac{9}{20}Y+Z$，

(3)$Y=\frac{13}{42}W+Z$，　　(4)$w=\frac{7}{12}(X+x)$，

(5)$x=\frac{9}{20}(Y+y)$，　　(6)$y=\frac{11}{30}(Z+z)$，　　[249]

(7)$z=\frac{13}{42}(W+w)$，　　(8)$W+x=$一个平方数，

(9)$Y+Z=$一个三角形数.

前七个方程较易求解，其答案是：

$W=10366482k$，　　$w=7206360k$，

$X=7460514k$，　　$x=4893246k$，

$Y=7358060k$，　　$y=3515820k$，

$Z=4149387k$，　　$z=5439213k$.

这里的 k 可取任意正整数值. 当 $k=1$ 时，即可求出满足首批七

---

① 阿基米德牛的问题是中国数学会第一任理事陈怀书先生首先引入中国的，其时间在本世纪30年代，见其著作《数学游戏大观》，商务印书馆出版. 但此书目前已成海内孤本. 读者们亦可参阅《100个著名数学问题：历史和解》，上海科技出版社，1982年第1版. 该书的德文原版在上海图书馆有收藏，书名 Hundert berühmte Probleme aus zwei Jahrtausenden mathematischer Kultur，德国 Heinrich Dörrie 著. 关于本问题的最新进展，则可参阅《马丁·加德纳全集》，该书有英、日文版本. ——译者注.

个条件的最小解，而得牛的总数为 50389082 头. 按照叙述本题条件的古代手稿，西西里岛的面积为 6358400 英亩，养活这些动物是可以做得到的.

第 8 个条件要求 $W+X=17826996k$ 是个平方数，这也容易满足. 由于 $17826996k$ 可分解为 $4\cdot 4456749k$，而较大的因子没有平方数的除数，足见 k 必须等于 $4456749t^2$，从而

$$W+X=4(4456749)^2t^2=79450446596004t^2$$

就可以是一个完全平方数了，但不幸的是，$Y+Z=51285802909803t^2$ 不是一个三角形数. 我们可以回忆起第 18 章讲过的内容，三角形数应具有 $n(n+1)/2$ 的形式，因而必须求解

$$51285802909803t^2=n(n+1)/2.$$

在方程两边乘上 8，再加 1，可得：

$$\begin{aligned}4n^2+4n+1=(2n+1)^2&=410286423278424t^2+1\\&=4729494(9314t^2)+1.\end{aligned}$$

若令 $2n+1=u$，$9314t=v$，我们即可得出

$$u^2-4729494v^2=1,$$

它是一个佩尔方程，这里 $D=4729494$，没有平方数除数，而 v 应能为 9314 整除.

本章后面要讲的连分数法可用来解此方程，但不妨请读者略为尝点味道，才能知道此项工作之艰巨：先来求一下，[250] $\sqrt{4729494}$ 的周期，然后是渐近分数的计算. 但是，1889年，无视摆在前面的困难，A・H・贝尔(Bell)，一位土木工程师，以及在一起创办伊利诺州希斯保罗市数学俱乐部的两位好朋友毅然进行了计算. 他们在这项工作上花费掉四年时间，终于算出了足足有 206531 位的数 t 的左边 32 位与右边 12 位. 这一 t 值是：

34555906354559370506303802963617

* * * * * 252058980100.

满足首批七个条件的数，每一个都要乘以 $k=4456749t^2$，最后结果如下：

W＝白的公牛数＝1596510804671144531435526194370

* * * * * 385150341800，

X＝黑的公牛数＝1148971387728289999712359821824

* * * * * 899825178600，

Y＝斑点公牛数＝1133192754438638077119555879202

* * * * * 921175894000，

Z＝黄的公牛数＝6390346482309028650085596761 83

* * * * * 635296026300，

w＝白的母牛数＝1109829892373319039723960215824

* * * * * 914059564000，

x＝黑的母牛数＝7535941420545426398144291195 89

* * * * * 238562645400，

y＝斑点母牛数＝5414608945714566780236199421 06

* * * * * 608963318000，

z＝黄的母牛数＝8376768824185244386922219841 07

* * * * * 116422113700.

总的牛数＝7760271406486818269530232833209

* * * * * 719455081800，

$W+X$＝一个平方数＝27454821923994345311478860161 94

* * * * * 284975520400，

$\sqrt{W+X}$＝1656949665133506668……357460163020，

$Y+Z$＝一个三角形数，T＝1772227402669540942128

11555385 * * * * * 556471920300，

$\sqrt{8T+1}$＝3765344502347205884……363134961201.

以上的每串星号表示 206502 位数码，带有星号的每行数目

字共有206544位或206545位数码.每串点号则代表103242位[251]数码.有点号的这两行各有103273位数码.假定每5个排成铅字占1英寸地位,则每一个206545位数字将大致长达$\frac{1}{3}$英里,完全印出上面的13个数目将需要一本2000页厚的大书.半径等于从地球到银河中心的一个球体也只能容纳得下这些动物中的极小一部分——不,即使它们是最小的微生物,甚至是电子.即使一千人在一起再干上一千年,能否完成贝尔的计算也颇成问题.然而,现代数字计算机在一段较合理的时间里可能完成此项工作.

读者在看了上面这一段以后,倒也不必为哈罗德及其萨克逊战士的问题犯愁——其答数比上面的问题要远远小得多.

*　　*　　*

早在很久以前的公元800年左右,印度人就懂得怎样解佩尔方程,但一直要等到伟大的数学家拉格朗日手里,才作出了完全而细致的分析,而这已经是在费马向瓦理斯与勃朗克两先生提出问题之后110年了.后面这两个人只是部分地解答了费马问题.拉格朗日的研究确实是数论领域中的一项突出成就.印度人婆罗摩笈多(Brahmagupta)在公元650年左右曾说过一句话:"在一年里头能解出方程$x^2-92y^2=1$的人是一位数学家."在那些日子里,他的确可以算上一个数学家,因为$x=1151$,$y=120$是方程的最小解.

*　　*　　*

值得指出一桩颇有兴味的事:怎样从$x^2-Dy^2=\pm1$的一组解导出无限多解.若p,q是满足方程$x^2-Dy^2=1$的最小值,则$x^2-Dy^2=1=p^2-Dq^2$.如果我们把方程的右边自乘到n次幂,由于$1^n=1$,当然其结果仍是1.于是有

$$x^2-Dy^2=(p^2-Dq^2)^n=1,$$

分解因子,得

$$(x+\sqrt{D}y)(x-\sqrt{D}y)=(p+\sqrt{D}q)^n(p-\sqrt{D}q)^n.$$

使具有同样运算符号的项相等，得：

$$x+\sqrt{D}y=(p+\sqrt{D}q)^n,$$
$$x-\sqrt{D}y=(p-\sqrt{D}q)^n.$$

[252]

把 x，y 解出来，我们就得到通解公式：

$$x=[(p+q\sqrt{D})^n+(p-q\sqrt{D})^n]/2, \quad \text{（公式 1）}$$
$$y=[(p+q\sqrt{D})^n-(p-q\sqrt{D})^n]/2\sqrt{D}, \quad \text{（公式 2）}$$

当 n 相继取值 1，2，3，…时，我们就可以随心所欲地得到许多不同解答.

例如解方程 $x^2-2y^2=1$，此时，最小解是 $3^2-2\cdot 2^2=1$，于是 $p=3$，$q=2$. 通解为

$$x=[(3+2\sqrt{2})^n+(3-2\sqrt{2})^n]/2,$$
$$y=[(3+2\sqrt{2})^n-(3-2\sqrt{2})^n]/2\sqrt{2}.$$

当 $n=1$ 时，得出 $x=3$，$y=2$，这便是第一个解答；当 $n=2$ 时，$x=17$，$y=12$，而 $17^2-2\cdot 12^2=1$，这是第二个解答；当 $n=3$ 时，$x=99$，$y=70$，而 $99^2-2\cdot 70^2=1$，这是第三个解答. 可以看到，n 增大时，x 与 y 的值增大得非常迅速.

类似地，$x^2-Dy^2=-1$（如果可能的话）的解也能求出，但这里，指数 n 必须永为奇数——例如，令它等于 $2m-1$. 在 $D=2$ 时，方程 $x^2-2y^2=-1$ 有一最小解 $p=1$，$q=1$. 于是，其通解为

$$x=[(1+\sqrt{2})^{2m-1}+(1-\sqrt{2})^{2m-1}]/2,$$
$$y=[(1+\sqrt{2})^{2m-1}-(1-\sqrt{2})^{2m-1}]/2\sqrt{2}.$$

当 $m=1$ 时，我们得到第一解 $x=1$，$y=1$；当 $m=2$ 时，$x=7$，$y=5$，$7^2-2\cdot 5^2=-1$ 是第二解；当 $m=3$ 时，$x=41$，$y=29$，41^2-

$2 \cdot 29^2 = -1$ 是第三解；……其他依此类推.

计算方程 $x^2 - Dy^2 = \pm 1$ 的最小解，虽然工作量有时也相当可观，但实际上并不存在真正困难. 许多计算家们已把结果列成表格形式，一直算到很大的 D 值. 在这种表格里，D 是不含有平方数因子的，因为平方数可以结合在 y 之中. 例如我们无需列出 $x^2 - 52y^2 = 1$ 的解，因为可将原方程改写为 $x^2 - 13(2y)^2 = 1$，只要把方程 $X^2 - 13Y^2 = 1$ 解出来，其中 Y 的偶数解就能给出我们所需的结果. 在婆罗摩笈多问题 $x^2 - 92y^2 = 1$ 中，满足方程 $x^2 - 23y^2 = 1$ 的 y 的偶数解就能得出所需结果.

D	x	y	D	x	y
2	3	2	30	11	2
3	2	1	31	1520	273
5	9	4	32	17	3
6	5	2	33	23	4
7	8	3	34	35	6
8	3	1	35	6	1
10	19	6	37	73	12
11	10	3	38	37	6
12	7	2	39	25	4
13	649	180	40	19	3
14	15	4	41	2049	320
15	4	1	42	13	2
17	33	8	43	3482	531
18	17	4	44	199	30
19	170	39	45	161	24
20	9	2	46	24335	3588
21	55	12	47	48	7
22	197	42	48	7	1
23	24	5	50	99	14
24	5	1	51	50	7
26	51	10	52	649	90
27	26	5	53	66249	9100
28	127	24	54	485	66
29	9801	1820	55	89	12

表 91　佩尔方程 $x^2 - Dy^2 = 1$ 的最小解

D	x	y	D	x	y
56	15	2	79	80	9
57	151	20	80	9	1
58	19603	2574	82	163	18
59	530	69	83	82	9
60	31	4	84	55	6
61	1766319049	226153980	85	285769	30996
62	63	8	86	10405	1122
63	8	1	87	28	3
65	129	16	88	197	21
66	65	8	89	500001	53000
67	48842	5967	90	19	2
68	33	4	91	1574	165
69	7775	936	92	1151	120
70	251	30	93	12151	1260
71	3480	413	94	2143295	221064
72	17	2	95	39	4
73	2281249	267000	96	49	5
74	3699	430	97	62809633	6377352
75	26	3	98	99	10
76	57799	6630	99	10	1
77	351	40	101	201	20
78	53	6	102	101	10

表 91　佩尔方程 $x^2-Dy^2=1$ 的最小解(续)　[254]

在 D 与满足方程的数目 p,q 的大小之间没有什么关系. 对某些 D 值来说, p,q 可能很小;而对于下一个 D 值,它们可变得出奇的大. 表 92 说明了这些变化. 满足方程 $x^2-1620y^2=1$ 的 x 只有 3 位;可是在 $x^2-1621y^2=1$ 里,它竟有 76 位之多! [253]

由 C・F・德根(Degen)作出计算,并于 1817 年刊行的《佩尔方程辞典》收入了方程 $y^2-Cx^2=1$ 的解,其中的 C 不包含平方数除数, C 值也不超过 1000. 此书经过许多研究者的校勘与推广,并对一些位数极多的特殊 D 值,计算了方程 $x^2-Dy^2=1$ 的解. 有一本很有趣味的书专门研究这一课题,叙述了它的历史,理论,给出了 $D=1501$ 到 2012 的解,这本书就是 E・E・惠

得福(Whitford)所编的《佩尔方程》.

D	x	y
1515	506	13
1516	33494917100186016050011 1891352199	860259161857394462507239 8763290
1546	3802792051	9671580
1597	519711527755463096224266 385375638449943026746249	130049860887907722503095 04643908671520836229100
1598	1599	40
1620	161	4
1621	629810181249373234303497 450009145781552994230866 705141285735231016966512 5001	156429324369979112128445 583345098338627552043874 824108399177922442751050 500
9781	476253760754326696229155 514206437758064174686478 459207091331165051639277 866110462913256334048166 314000750317798423947886 553290523568954482295429 78234993801	481555989037307915758858 176980967932471259067113 218060716438458121121697 033150997478138226408634 091745993475126174622767 474943622729435256180363 7330579140

表 92 佩尔方程 $x^2-Dy^2=1$ 的最小解(很大的值)

* * *

48 这个数有一个很奇特的性质,如果把 1 加到它上面,和数将是一个平方数 49;如果把 1 加到它的一半上去,结果仍将是一个平方数 25. 还有什么其他数也有类似性质呢? 设此数为 b,于是有 $b+1=x^2$,$\frac{b}{2}+1=y^2$. 消去 b 后,可得 $x^2-2y^2=-1$,而这是一个佩尔方程. 从最小解 $x=1$,$y=1$,$b=0$ 出发,我们可以像以前那样得出方程的一些其他解,表 93 给出了显示此种特异性质的前 9 个 b 数.

[255]

第 14 章中我们讨论了两直角边 m^2-n^2 与 $2mn$ 相差为 1 的毕氏三角形. 它要求 $m^2-n^2-2mn=\pm1$,即 $(m-n)^2-2n^2=\pm1$,而这是一个佩尔方程. 相继的毕氏三角形可以交替地从方

x	y	x^2	y^2	$b=2y^2-2$ $=x^2-1$
1	1	1	1	0
7	5	49	25	48
41	29	1681	841	1680
239	169	57121	28561	57120
1393	985	1940449	970225	1940448
8119	5741	65918161	32959081	65918160
47321	33461	2239277041	1119638521	2239277040
275807	195025	76069501249	38034750625	76069501248
1607521	1136689	2584123765441	1292061882721	2584123765440

表 93　$x^2-2y^2=-1$ 的解

程 $(m-n)^2-2n^2=+1$ 与 $(m-n)^2-2n^2=-1$ 分别导出. 由 $1^2-2\cdot 1^2=-1$，有 $n=1$，$m-n=1$，$m=2$. 与此对应的毕氏三角形 $3^2+4^2=5^2$ 的两条直角边分别为 $m^2-n^2=3$，$2mn=4$. 而从 $3^2-2\cdot 2^2=+1$ 有 $n=2$，$m-n=3$，$m=5$，与此相应的毕氏三角形 $20^2+21^2=29^2$ 的两条直角边却是 $m^2-n^2=21$ 与 $2mn=20$.

由于佩尔方程 $x^2-2y^2=\pm 1$ 中 x 与 y 的通解是

$$x=[(1+\sqrt{2})^r+(1-\sqrt{2})^r]/2,$$
$$y=[(1+\sqrt{2})^r-(1-\sqrt{2})^r]/2\sqrt{2},$$

从而可以求出 $m=x+y$ 与 $n=y$ 的通解，接着，又能求得 $X=m^2-n^2=x^2+2xy$，$Y=2mn=2xy+2y^2$，$Z=m^2+n^2=x^2+2xy+2y^2$，它们是毕氏三角形的三条边，最后我们将得出： [256]

$$X_r=\frac{(\sqrt{2}+1)^{2r+1}-(\sqrt{2}-1)^{2r+1}}{4}+\frac{1}{2}(-1)^r,$$

$$Y_r=\frac{(\sqrt{2}+1)^{2r+1}-(\sqrt{2}-1)^{2r+1}}{4}-\frac{1}{2}(-1)^r,$$

$$Z_r=\frac{(\sqrt{2}+1)^{2r+1}+(\sqrt{2}-1)^{2r+1}}{2\sqrt{2}},$$

这就是第 14 章中给出的直角边是连续数的毕氏三角形三条边

的公式.

* * *

多半是在大吃大喝之后但总算尚不碍事,你可曾梦见过自己在盘旋曲折的过道里爬行而最后竟然闯入了马克斯费尔德·帕里什(Maxfield Parrish)建造的神仙世界? 与此相仿,人们在遭遇"渐近分数"、"部分商"、"连分数"之后总会产生一种异样感觉,自己终于涉足到佩尔方程的奇异的丢番图王国,在那个地方,二次根式以周期链的形式风行一时.

涉及连分数的一些规则非常笨重而难记,但由此所导得的结果,例如佩尔方程的解等等则是十分有趣的,这就充分表明了它们的存在价值以及所以要在这里加以介绍的原因. 一个简单连分数具有如下形式:

$$a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{a_4+\cdots}}}$$

为了简便起见,通常也可记为:

$$a_1+\frac{1}{a_2}+\frac{1}{a_3}+\frac{1}{a_4}+\cdots.$$

近年来它有时也用$(a_1,a_2,a_3,a_4,\cdots)$来表示.

任何数目都可写成一个简单连分数. 所谓"简单",那是因为[257]所有的分子都是1. 当数为有理数,即可表示为两个整数之商时,连分数是有尽的;但当数为无理数时,连分数出现周期性,后面这一点与无理数的小数表示大不相同——它们永不循环. 例如$\sqrt{3}$是一个无理数,它等于1.732051…,不论多少位数码,它都不会出现周期性重复.

用了连分数之后,有理数$\frac{40}{17}$可记为

$$\frac{40}{17}=2+\frac{1}{2}+\frac{1}{1}+\frac{1}{5}.$$

而无理数

$$\sqrt{19}=4+\frac{1}{2}+\frac{1}{1}+\frac{1}{3}+\frac{1}{1}+\frac{1}{2}+\frac{1}{8}+\frac{1}{2}+\frac{1}{1}$$
$$+\frac{1}{3}+\frac{1}{1}+\frac{1}{2}+\frac{1}{8}+\frac{1}{2}+\cdots;$$
$$\sqrt{2}=1+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}+\cdots.$$

甚至数学家们也经常避开连分数，他们宁可多走一些迂回曲折的路来避开它，而不愿深入渐近分数妖怪经常出没的地下洞穴. 我们当然也不想在那里逗留而只是急急忙忙地过路，冒着不时要同一个不可避免的妖精厮打的风险.

人们或许把之所以不愿使用连分数的原因，归咎于分母的摇摆不定. 例如，在$\frac{40}{17}$的连分数表达式中，前两项之和 $2\frac{1}{2}$是大于$\frac{40}{17}$的，因为在其分母上少了$\frac{1}{1}$所带来的增量；另一方面，$2+\frac{1}{2}+\frac{1}{1}=2\frac{1}{3}$却又小于$\frac{40}{17}$，因为分数$\frac{1}{1}$在其分母上又少了$\frac{1}{5}$这个增量，有了它才能使分数比 $2\frac{1}{2}$小一点而比 $2\frac{1}{3}$大一点. 现在总算安定了吧！

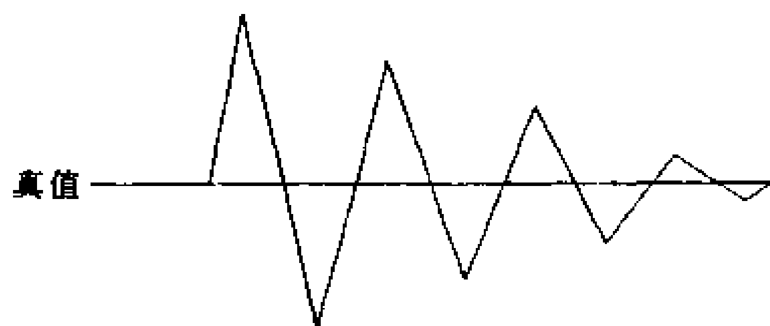
如果我们遇到数$\frac{40}{17}$或 $\sqrt{19}$，我们怎样把它们展为连分数呢？这是第一个问题.

另外，有理数的连分数表达式只有有限项，只要从右边化简连分数，人们就可以得到原来的数目. 另一方面，$\sqrt{19}$之类的无理数将展为无限连分数，人们不可能站在连分数系列的尽头进行化简. 为了方便起见，只好从第一项开始，考虑有限项的和. 这 [258]

样的"和"称为渐近分数.它是一个有理数,也是无理数真值的一个近似.在无理数已展为循环连分数之后,怎样计算渐近分数?这是第二个问题.

这两个问题解决起来都很费手脚,现有一些较为简单的规则可供使用,以避免繁复的计算.但是,人们为什么要自找麻烦呢?那是由于渐近分数之间存在着一些奇妙关系,可用来解决诸如 $119x-32y=1$ 或 $x^2-13y^2=1$ 此类的一次或二次丢番图方程.这又是一个实际例子,能说明数学里头表面上毫无关系的东西实际上能以出人意外与美妙的方式紧密联系.为了领略这些工具的威力,建议读者在往下阅读之前,解一下较简单的二次不定方程 $x^2-211y^2=1$ 的整数解.†

在连分数的分母上不断增加分母,我们在每一步得到的表达式,将是交替地大于或小于数的真值.对有理数来说,最终会到达其真值;但对无理数却是永远到不了.不过,在每一步,渐近分数将越来越接近于真值.



[259] 图 23 渐近分数越来越接近于真值

要把$\frac{119}{32}$展成连分数,先做除法,得出 $3\frac{23}{32}$.然后把$\frac{23}{32}$变为$\frac{32}{23}$,继续做除法,得出 $1\frac{9}{23}$.照此继续进行下去,$\frac{23}{9}=2\frac{5}{9}$,$\frac{9}{5}=1\frac{4}{5}$,$\frac{5}{4}=1\frac{1}{4}$,$\frac{4}{1}=4$.每一次商的整数部分是连分数的分母 a_1,a_2,a_3,…,当商是一个整数时,运算就终止了.于是 $a_1=3$,$a_2=$

$1, a_3=2, a_4=1, a_5=1, a_6=4$.

$$\frac{119}{32}=3+\frac{1}{1+}\frac{1}{2+}\frac{1}{1+}\frac{1}{1+}\frac{1}{4}.$$

由于 119/32 是一个有理数，因而在有限次除法之后，整数商必然要出现. 倘若我们从 32/119 开始，则结果将是 $a_1=0, a_2=3$, $a_3=1, a_4=2, a_5=1, a_6=1, a_7=4$，于是

$$\frac{32}{119}=\frac{1}{3+}\frac{1}{1+}\frac{1}{2+}\frac{1}{1+}\frac{1}{1+}\frac{1}{4}.$$

现在来看渐近分数. 它们可分别由连分数的前一项，前二项，前三项，……求和而得. 相应的结果是 3/1，4/1，11/3，15/4，26/7，119/32. 它们交替地小于或大于 119/32，每一个渐近分数都比它的前一个更为接近真值.

由前两个渐近分数与 a_i 值求第 n 个渐近分数有一个简单得多的办法，那便是应用公式：

$$p_n=a_np_{n-1}+p_{n-2}, \qquad (公式 3)$$

$$q_n=a_nq_{n-1}+q_{n-2}. \qquad (公式 4)$$

例如，上例的第四个渐近分数 15/4 可从 $a_4=1, p_3=11, q_3=3$, $p_2=4, q_2=1$ 算出：

$$p_4=1\cdot 11+4=15,$$

$$q_4=1\cdot 3+1=4.$$

第一个、第二个渐近分数 p_1/q_1，p_2/q_2 当然不能从其前两个渐近分数算得. 但作为其替代办法，任何情况下都存在着下列关系：

$$q_1=1, \ p_1=a_1, \ q_2=a_2, \ p_2=a_2a_1+1.$$

因而前两个渐近分数永远是

[260] $a_1/1$ 与 $(a_1a_2+1)/a_2$.

可以用列表的办法来计算连分数的一系列渐近分数，当然各个 a_i 还是要用除法算出来，至于 p_i、q_i 以及一系列的收敛分数，那就可以用递推公式迅速算出.

例如我们要把 426/359 展为连分数并求出一系列收敛分数. 首先通过除法求出各个 a_i，然后利用公式 3，4，造出表 94.

n	1	2	3	4	5	6	7
a_n	1	5	2	1	3	1	4
p_n	1	6	13	19	70	89	426
q_n	1	5	11	16	59	75	359

表 94 把 426/359 展为连分数

于是

$$\frac{426}{359}=1+\frac{1}{5}+\frac{1}{2}+\frac{1}{1}+\frac{1}{3}+\frac{1}{1}+\frac{1}{4},$$

而各渐近分数为

1/1，6/5，13/11，19/16，70/59，89/75，426/359.

* * *

由二次不尽根 $\sqrt{D}$ 展为连分数并由此求出各个收敛分数的步骤要长一些，但由于从收敛分数可导出佩尔方程的可贵解法，这些额外劳动还是很值得的. 此时，各渐近分数 p_n/q_n 仍可从 $a_1, a_2, a_3, \cdots$ 进行计算，使用的公式与有理数的情况完全一样. 但各个 a_i 的定义有所不同，它们的计算需要另一套公式，并包括两个额外引进的数量 P 与 Q，其定义如下：

$P_1=0$,

$Q_1=1$,

a_1 是 $\sqrt{D}$ 的整数部分，

$P_2 = a_1,$

$Q_2 = D - a_1^2,$

$P_n = a_{n-1}Q_{n-1} - P_{n-1},$ （公式5）

$Q_n = (D - P_n^2)/Q_{n-1},$ （公式6）

a_n 是$(a_1 + P_n)/Q_n$ 的整数部分. [261]

为了方便起见，这里把公式3,4重复一下：

$p_n = a_n p_{n-1} + p_{n-2},$

$q_n = a_n q_{n-1} + q_{n-2},$

$q_1 = 1,\ p_1 = a_1,\ q_2 = a_2,\ p_2 = a_2 a_1 + 1.$

利用这些公式、规则，我们即可把 $\sqrt{23}$展为连分数，并造出表95.

n	1	2	3	4	5	6	7	8	9	10
P_n	0	4	3	3	4	4	3	3	4	4
Q_n	1	7	2	7	1	7	2	7	1	7
a_n	4	1	3	1	8	1	3	1	8	1
p_n	4	5	19	24	211	235	916	1151	10124	11275
q_n	1	1	4	5	44	49	191	240	2111	2351

表95 把 $\sqrt{23}$展为连分数

于是

$$\sqrt{23}=4+\frac{1}{1}+\frac{1}{3}+\frac{1}{1}+\frac{1}{8}+\frac{1}{1}+\frac{1}{3}+\frac{1}{1}+\frac{1}{8}+\frac{1}{1}+\cdots\frac{1}{+a_n}+\cdots.$$

我们对 p_i, q_i 如此操心，现在总算到了收获季节. a_i 与 P_i 不过是到达终点的工具，就像是稻壳一样要被风刮走，剩下来的只是有营养价值的谷粒 p_i, q_i 与 Q_i. 连分数里头有两个十分重要的关系式：

$p_n q_{n-1} - p_{n-1} q_n = (-1)^n,$ （公式A）

$p_n^2 - D q_n^2 = (-1)^n Q_{n+1}.$ （公式B）

用公式 A 可解线性不定方程 $ax-by=\pm1$；用公式 B 则可求出佩尔方程 $x^2-Dy^2=\pm1$ 的解. 解线性方程时，可先把 a/b 展为连分数，则从最后一个算起，倒数第二个渐近分数 $(p_{n-1})/(q_{n-1})$ 的分子 p_{n-1} 就是 y 值；而分母 q_{n-1} 就是 x 值. 最后一个渐近分数 p_n/q_n 当然是 a/b，这里 $p_n=a$，$q_n=b$.

设我们要求方程 $119x-32y=1$ 的正整数解. 我们在上文已把 119/32 展成连分数，并发现第五个，亦即倒数第二个渐近分数是 26/7. 于是 $p_{n-1}=y=26$，$q_{n-1}=x=7$，并且 $119\cdot7-32$ [262] $\cdot26=(-1)^6=+1$.

其他解可在表达式 $x=7+32K$；$y=26+119K$ 中指定 K 为任意整数值而得. 例如，$K=1$ 时，便得 $x=39$，$y=145$，且有 $119\cdot39-32\cdot145=1$.

若我们从 $32x-119y=1$ 开始，则我们可在 32/119 的连分数展式中求出 $p_{n-1}=7=y$，$q_{n-1}=26=x$，此时有 $32\cdot26-119\cdot7=(-1)^7=+1$. 为了得到结果为 +1 的解，可在每一项上乘以 −1，即

$$32(-26)-119(-7)=+1.$$

记住 $-26+119K$ 是 x 的通解式，而 $-7+32K$ 是 y 的通解式，由此即可获得正整数解. 令 $K=1$，则 $x=93$，$y=25$，且 $32\cdot93-119\cdot25=1$.

解线性不定方程 $ax-by=-1$ 时，也可类似地进行.

* * *

现在回到公式 B，我们可通过表 95 来验证这个关系式. 例如，$n=2$ 时，$p_2=5$，$q_2=1$，$Q_3=2$，此时有 $5^2-23\cdot1^2=+2$. 再看 $n=5$，则 $p_5=211$，$q_5=44$，$Q_6=7$，且有关系 $211^2-23\cdot44^2=-7$. 当 $Q_{n+1}=+1$ 时，我们即得出著名的佩尔方程，

$$p_n^2-Dq_n^2=(-1)^n(1), \qquad \text{(公式 C)}$$

或者更简单地写成

$$x^2 - Dy^2 = (-1)^n = \pm 1.$$

这里的 n 是使 Q_{n+1} 等于 1 的那个下标值. 数 D 是设定为除 1 外不含其他平方数除数的,若它原来含有的话,则可视为包括在 y^2 中的一部分而除去.

表 95 显示出:在 a_n 等于 a_1 的二倍以后,表中的 a_i,p_i 与 Q_i 出现周期性重复现象. 这情况永远为真. 相应的 Q 项,即 Q_n 于是永远等于 1. 例如,在表中,可以看到 $a_5=8$,它是 $a_1=4$ 的二倍;于是 a_6 同 a_2 一样,a_7 同 a_3 一样,……如此等等. 另外还有 $Q_5=1$. 从而 $p_4^2-Dq_4^2=24^2-23\cdot5^2=(-1)^4=1$. 由于 Q_9 也等于 1,于是 $p_8^2-Dq_8^2=1151^2-23\cdot240^2=(-1)^8=+1$;同样,$Q_{13}$,$Q_{17}$,…,$Q_{4k+1}$也与此类似. 因为 Q 每经过 r 项就周期性地取 1 值,于是我们可把公式 C 推广为如下形式:

$$p_{rk}^2 - Dq_{rk}^2 = (-1)^{rk}, \qquad (\text{公式 D})$$

这里,k 是任何正整数. [263]

此式表明,r 为奇数时,$x^2-Dy^2=+1$ 或 $x^2-Dy^2=-1$ 的解可分别从 k 被选为偶数或奇数而得出. 但若 r 为偶数,则没有一个 k 值能使指数成为奇数,因而在那种情况下,方程 $x^2-Dy^2=-1$ 无解.

作为实例,让我们来看方程 $x^2-13y^2=-1$,首先通过列表,把与 $\sqrt{13}$有关的数据都算出来. 接着,算出渐近分数 $p_5/q_5=18/5$,以及 $Q_6=1$.

n	1	2	3	4	5	6	7	8	9	10	11
P_n	0	3	1	2	1	3	3	1	2	1	3
Q_n	1	4	3	3	4	1	4	3	3	4	1
a_n	3	1	1	1	1	6	1	1	1	1	6
p_n	3	4	7	11	18	119	137	256	393	649	
q_n	1	1	2	3	5	33	38	71	109	180	

表 96 把 $\sqrt{13}$展为连分数

于是 $p_5^2-13q_5^2=18^2-13\cdot5^2=(-1)^5=(-1)$. 然后我们应用公式 D,令 k 为任一偶数,譬如说 $k=2$. 于是有

$$p_{10}^2-13q_{10}^2=(-1)^{10}=+1;$$

而事实上的确有:

$$649^2-13\cdot180^2=+1.$$

另一方面,方程 $x^2-13y^2=-1$ 的解也可从 k 为奇数时导出:譬如说 $k=1$ 时,从关系式 $18^2-13\cdot5^2=-1$ 可以立即把解写出来.

现在,读者们也许已经跃跃欲试,想去解一解在本章前面部分已经提到过的方程 $x^2-211y^2=1$ 了,自然要求出 $\sqrt{211}$ 的渐近分数,还得有充分耐心,因为 $Q_{n+1}=1$ 可能姗姗来迟——但请放心,它终究是会来的.†

*　　　*　　　*

由一般关系式 $p_n^2-Dq_n^2=(-1)^2Q_{n+1}$ 可导出方程 $x^2-Dy^2=\pm c$ 的解,但 c 必须小于 $\sqrt{D}$,而且 c 须为 $\sqrt{D}$ 的渐近分数中周期里头的某个 Q_i,由此可见,D 与 c 并不能任意选取. 若 $c>\sqrt{D}$,则解法就显得相当复杂,人们还是暂时退却一下为好. 克里斯多的代数教科书将为大无畏的数学西格弗里德(Siegfried)①熔铸宝剑来进攻妖怪. 但若已知其一个解,则可以算出其他无限多解,但不像方程右边为±1 时那么轻而易举. [264]

以第一解为基础,乘上 $x^2-Dy^2=\pm1$(称为右端是单位形式的方程)的任一解. 然后适当安排乘积各项,即可得出所需的其他解. 若 p,q 满足方程 $x^2-Dy^2=+c$ 或 $-c$,而 r,s 满足方程 $x^2-Dy^2=+1$ 或 -1,那就有

① 西格弗里德是德国 13 世纪初民间史诗《尼伯龙根之歌》中的英雄人物,能擒妖降魔. 瓦格纳为此而创作了歌剧. ——译者注.

$$(p^2 - Dq^2)(r^2 - Ds^2) = +c \text{ 或 } -c;$$

把左端乘出并重新集项后，我们就可得出：

$$(pr \pm Dqs)^2 - D(ps \pm qr)^2 = +c \text{ 或 } -c.$$

举例如下：设要求出

$$x^2 - 13y^2 = +3$$

的好几个解，先看表 96，由于 3 是 Q_n 中的一个，表明它是有解的，最小解是 $4^2-13\cdot 1^2=3$. 另外，前已说过，方程 $x^2-13y^2=+1$ 的最小解是 $649^2-13\cdot 180^2=+1$，从而 $p=4, q=1, r=649, s=180$，并有如下关系式成立：

$$(4\cdot 649 \pm 13\cdot 1\cdot 180)^2 - 13(4\cdot 180 \pm 1\cdot 649)^2 = 3,$$

由此可得

$$4396^2 - 13\cdot 1369^2 = 3$$

以及

$$256^2 - 13\cdot 71^2 = 3.$$

另外，从关系式 $7^2-13\cdot 2^2=-3$（再次参阅表 96）以及 $649^2-13\cdot 180^2=+1$ 可以推出

$$9223^2 - 13\cdot 2558^2 = -3$$

以及

$$137^2 - 13\cdot 38^2 = -3.$$

[265]

利用右端为负的单位形式，再结合考虑 $18^2-13\cdot 5^2=-1$，$4^2-13\cdot 1^2=+3$ 两关系式，即可导出

$$137^2 - 13\cdot 38^2 = -3$$

以及

$$7^2 - 13\cdot 2^2 = -3.$$

若将负单位形式与 $7^2-13\cdot2^2=-3$ 结合起来考虑则可得出

$$256^2-13\cdot71^2=+3$$

以及

$$4^2-13\cdot1^2=+3.$$

最后要说上一句，可利用单位形式的乘幂来得出其他许多解，要多少有多少.

*　　　*　　　*

在公式 6 中提到过的关系式 $Q_n=(D-P_n^2)/Q_{n-1}$ 可用来推求 D 的一系列平方剩余，正如在第 21 章中讲到的，这个信息在把数 D 分解因子时可能相当有用. 把上面的表达式去分母，可得

$$P_n^2-D=-Q_nQ_{n-1}，也就是\ P_n^2\equiv-Q_nQ_{n-1}\ \mathrm{mod}\ D.$$

它意味着，$-Q_nQ_{n-1}$ 是 D 的一个平方剩余. 但我们回想起 Q_1 恒等于 1；因此 $-Q_2$ 应是 D 的一个平方剩余. 同样，$-Q_2Q_3$ 也是平方剩余，既然 $-Q_2$ 是个平方剩余，可见 Q_3 肯定也是. 最后的结论是：带有奇数下标的一切 Q_i 以及带有偶数下标的 Q_i 的相反数都是 D 的平方剩余.

可以把上述规则应用到表 96 中由 $\sqrt{13}$ 导出的各个 Q_i 值，这时有，$Q_1=1$，$Q_2=4$，$Q_3=3$，$Q_4=3$，$Q_5=4$，$Q_6=1$，等等，而 1，3，4，−4，−3，−1 统统都是 13 的平方剩余. 但要注意，这个方法并不是永远都能给出某个模数的全部平方剩余的，譬如说，应用表 95 只能得出模 23 的 11 个平方剩余中的 3 个，但对位数众多的很大的 D 来说，它毕竟能够提供个数足够多的、较小的平方剩余数，而这已经可以极大地减轻把 D 分解为质因数的沉重负担. 另外，也不要忘记，作为真正的平方剩余，求出来的每个 Q_i 值都应当与 D 互质，所以，用这种方法求出的任何 Q_i 值都必[266]须经过互质性测试.

在求解线性与二次丢番图方程时表现出来的优美与用处，以求在分解因数时连分数所能提供的帮助，我们已经讲得足够

多了.它不愧为数论领域中为数寥寥无几的直接方法之一.

参考文献

Archibald, R. C. "Cattle Problem of Archimedes," *American Mathematical Monthly*, **25**(1918), 411.

Barlow, P. *Theory of Numbers*. London: J. Johnson & Co., 1811.

Bell, A. H. "'Cattle Problem.' By Archimedes 251 B. C.," *American Mathematical Monthly*, **2**(1895), 140.

——. "Cattle Problem of Archimedes," *Mathematical Magazine*, **1**(1882—1884), 163.

Cajori, F. *A History of Mathematics*. New York: Macmillan Co., 1919.

Carmichael, R. D. *Theory of Numbers and Diophantine Analysis*. New York: Dover Publications, Inc., 1959.

Chrystal, G. *Textbook of Algebra*. 2 vols. New York: Dover Publications, Inc., 1961.

Cunningham, A. *Quadratic Partitions*. London: F. Hodgson, 1904.

Degan, C. F. *Canon Pellianus*. Copenhagen, 1817.

Dickson, L. E. *History of the Theory of Numbers*. 3 vols. New York: Chelsea Publishing Co., 1950.

Dudeney, H. E. *Amusements in Mathematics*. New York: Dover Publications, Inc., 1958.

Evans, A. B., and Hart, D. S. "Problem: [To Find the Least Integral Solution of $x^2-953y^2=\pm 1$]," *Mathematical Questions from the Educational Times*, **23**(1875), 107.

Lehmer, D. N. *Factor Stencils*. Washington, D. C.: Carnegie Institution of Washington, 1939.

Licks, H. E. *Recreations in Mathematics.* New York: D. Van Nostrand Co., 1921.

Martin, A. "Solution to Problem: Find the Least Integral Values of x and y That Will Satisfy the Equation $x^2-9817y^2=1$," *The Analyst*, **4**(1877), 154.

——. "An Error in Barlow's 'Theory of Numbers,'" *Bulletin of the Philosophical Society of Washington*, **11**(1888), 592.

——. "Solution of Problem: [$x^2-5658y^2=1$ in Integers]," *Mathematical Questions from the Educational Times*, **26** (1876), 87.

——. "Solution to Problem: Find the Least Integral Values of x and y That Will Satisfy the Equation $x^2-9781y^2=1$," *Mathematical Visitor*, **1**(1877—1881), 26.

Martin, A., and Hart, D. S. "Solution to Problems: [$241x^2+67x=1$ Is a Square; $953z^2+87z+1$ Is a Square; the Least Values That Will Make $x^2-5693y^2=-1$]," *Mathematical Questions from the Educational Times*, **25**(1876), 97. [267]

Merriman, M. "Cattle Problem of Archimedes," *Popular Science Monthly*, **67**(1905), 660.

Whitford, E. E. *Pell Equation.* New York: Columbia University Press, 1912.

Wright, H. N. *First Course in Theory of Numbers.* New York: J. Wiley & Sons, 1939.

Young, J. W. A. *Monographs on Topics of Modern Mathematics.* New York: Dover Publications, Inc., 1955. [268]

第23章 形 态 学

数字世界的漫游者现在已走近几乎无法入内的形态王国的前哨阵地. 我们的周围全是形状怪异，莫可名状的模糊阴影，暗无天日. 稠密而穿不透的大气形成了三元二次型与四元三次型. 这里，导游服务是绝对必要的，我们的一大堆问题几乎把他淹没. 他告诉我们一些王国领导人的名字，最前头的是拉格朗日与勒让德，接着是令人敬爱的卡尔·弗里德列希·高斯，我们也听到了戴德金(Dedekind)与克莱因(Klein)的二元二次型，庞加莱(Poincaré)的多才多艺，还有狄利克莱(Dirichlet)，厄米特(Hermite)，克朗尼克(Kronecker)，凯莱(Cayley)，雅可比，史密斯(Smith)等人的许多发现——我们很快就忘记了这些名字，他们实在太多.

导游所使用的词汇也使我们感到迷惑不解——自形与多形，单形与示性数，正常与异常等价关系，……听起来像是没完没了，简直同外国语那样晦涩难懂.

*　　　*　　　*

形式理论属于内在艰深课题的最困难分支之一. 几乎在所有的数学分支中都有它的衍生物. 在我们的简单游历中只能介绍一些最粗浅的内容.

现在先取一个两平方数的和，例如 $1^2+2^2=5$. 把此数乘以另外两个平方数的和；例如 $2^2+7^2=53$. 则乘积 265 也是两平方数之和，即 16^2+3^2 或 12^2+11^2. 平方和与平方和的乘积仍旧是

平方和：

$$(x^2+y^2)(a^2+b^2)=(ax+by)^2+(bx-ay)^2$$
$$=(ax-by)^2+(bx+ay)^2.$$

婚生子女能继承他们父母的气质，数学上这种例子很多，以上仅[269]其一例而已.

更值得注意的是三项式的关系，它包含了上例为其特款. 即：

$$(x^2+axy+by^2)(t^2+atu+bu^2)=r^2+ars+bs^2.$$

这里，a，b 是给定的常数，它告诉我们，如果 M 与 N 可分别表示为 $x^2+axy+by^2$ 与 $t^2+atu+bu^2$，则总能找到两个整数 r，s，以使得乘积 MN 等于 $r^2+ars+bs^2$. 这两个整数可从下列关系式中求出：

$$r=xt-byu,$$
$$s=yt+xu+ayu.$$

设 $x=4$，$y=3$，$t=2$，$u=1$，a，b 分别为 7 与 5，则 $M=4^2+7\cdot 4\cdot 3+5\cdot 3^2=145$，$N=2^2+7\cdot 2\cdot 1+5\cdot 1^2=23$. 于是 $MN=145\cdot 23=3335$，而此数可通过同样的 a，b 与 r，s 来表达.（这里，$r=4\cdot 2-5\cdot 3\cdot 1=-7$，$s=3\cdot 2+4\cdot 1+7\cdot 3\cdot 1=31$.）也就是$(-7)^2+7(-7)(31)+5\cdot 31^2$.

第 22 章中讲到佩尔方程

$$x^2-Dy^2=1.$$

由此类方程的两个解，通过如下关系式

$$(x_1^2-Dy_1^2)(x_2^2-Dy_2^2)=(x_1x_2+Dy_1y_2)^2-D(x_1y_2+x_2y_1)^2=1$$

可求出其解. 这又是一个实例，表明某种形式的两个表达式的乘积依然能得出同一形式的表达式. 例如从佩尔方程的两个解 $4^2-15\cdot 1^2=1$ 以及 $31^2-15\cdot 8^2=1$，可以得出另外一个解：

$$244^2 - 15 \cdot 63^2 = 1.$$

下列关系式同样也成立,即:

$$(x_1^2 - Dy_1^2)(x_2^2 - Dy_2^2)$$
$$= (x_1x_2 - Dy_1y_2)^2 - D(x_1y_2 - x_2y_1)^2.$$

类似地还有,

$$(x_1^2 + Dy_1^2)(x_2^2 + Dy_2^2)$$
$$= (x_1x_2 \pm Dy_1y_2)^2 + D(x_1y_2 \mp x_2y_1)^2.$$

* * *

二元二次型 $ax^2+bxy+cy^2$ 已投入很大力量并引起广泛注意,因为通过它可以判定能表示成此种形式能否分解因子,或者认定它为素数.我们已经知晓,如果一个奇数只能用一种方法表为两个互质的平方数之和,则它必为素数或素数的某次乘方.第21章里头已讲过,当一数 N 能用两种或更多种方法表为两个平方数之和,或者 N 能用两种或多种方法表为 x^2+Dy^2 时,如何把 N 分解因子的办法.这些方法可以通过深奥难解但却引人入胜的思索而进一步大大扩展. [270]

如果数 N 只能用一种方法表示为 x^2+Dy^2,x^2 与 Dy^2 互质,且 D 不超过 10,或者对某些较大的 D 值,则 N 必为一个素数,或素数的乘幂,或上述数量的二倍.换言之,若一合数能表示为 x^2+Dy^2,其中 x^2 与 Dy^2 互质,而 D 不超过 10,则必至少还有一种方法来把该合数表示为上述形式.例如 $D=7$、$x=5$,$y=3$ 时有 $N=5^2+7\cdot3^2=88$,由于 88 是合数,且 5^2 与 $7\cdot3^2$ 互质,则可以肯定至少还有一种方法把 88 表示为一个平方数与另一平方数的七倍之和.实际上也确乎如此,这是由于 $88=9^2+7\cdot1^2$ 之故.如果我们另取一数 $8^2+7\cdot3^2=127$,并已知道 127 是个素数,则我们就可以肯定,再也不存在另外一种办法来把此数表示为 x^2+7y^2 的形式.再看一例,$14=3^2+5\cdot1^2$,尽管 14 是个合

数，但它却是某个素数的二倍（$14=2\cdot7$），所以还是不存在另一种办法可把它表示为 x^2+5y^2 的形式.

即便是合数，它仍然只能存在一种方式把它表示为 x^2+Dy^2 的形式，D 的这种最小值是 11. 此时，不论该数是否为素数，素数的乘幂，以上数量的二倍，以及两项是否互质. 此等因素，对它全无影响. 例如，在 $69=5^2+11\cdot2^2$ 中，两项是互质的，69 并非素数或素数的乘幂；可是不存在另一种办法来把 69 表示为 x^2+11y^2.

当一整数只能用一种方法表示为 x^2+Dy^2（或 x^2-Dy^2）时，称之为单形；表示法不止一种时，称为多形. 迄今为止，已知只有 65 个 D 值得以断定，呈单形的数必为素数，素数的乘幂，或以上各数量的二倍.

表 97 中给出的这 65 个正整数称为"示性数". 在 100,000 以下，再也没有别的示性数了. 对表中没有列举出来的 D 值，例如 11，14，17，19，20 等等，数 x^2+Dy^2 即使是单形或合数，仍有可能不是素数的乘幂或它的二倍.

[271]

1	16	48	120	312
2	18	57	130	330
3	21	58	133	345
4	22	60	165	357
5	24	70	168	385
6	25	72	177	408
7	28	78	190	462
8	30	85	210	520
9	33	88	232	760
10	37	93	240	840
12	40	102	253	1320
13	42	105	273	1365
15	45	112	280	1848

表 97 正示性数

在判定一个数是否素数时，示性数是很有用的. 例如我们已通过什么其他办法，把数 $N=1132861$ 表示为 $1043^2+93\cdot22^2$. 由于 93 是列在表中的示性数，所以如果 N 不能用其他方式表

示为 x^2+93y^2，则它肯定是素数或素数的某个乘幂. 若将 N 除以 93，得商 12181+，这表明 y 不可能大于 12181 的平方根，亦即 110. 这样一来就易于查验清楚，不可能有 x，y 的其他值来满足上述表达式，于是就能断定 N 必是一个素数或素数的某个方幂. 但若 93 不是示性数，那么即便 N 是单形，仍然不足以判定它的性态.

*　　　　*　　　　*

某些整数 N 能同时表示为 x^2-Dy^2 与 $Dx_1^2-y_1^2$ 两种形式. 这种数称为"反形数". 使其为可能的 D 值是那种能使佩尔方程

$$x_n^2 - Dy_n^2 = -1$$

有解的 D 值. 例如，由于 $x^2-13y^2=-1$ 有解，任何一个可表作 x^2-13y^2 的数肯定也可表示为 $13x_1^2-y_1^2$. 由于 $x_n^2-7y_n^2=-1$ 无解，所以 x^2-7y^2 不能转化为 $7x_1^2-y_1^2$. 在能转化的情况下，它可以通过以下关系来实现：

$$\begin{aligned} N = x^2 - Dy^2 &= -(x^2 - Dy^2)(x_n^2 - Dy_n^2) \\ &= D(xy_n - yx_n)^2 - (xx_n - Dyy_n)^2 \\ &= D(xy_n + yx_n)^2 - (xx_n + Dyy_n)^2. \end{aligned}$$

[272]

作为一个实例，$x_n=18$，$y_n=5$ 是 $x_n^2-13y_n^2=-1$ 的一个解. 现取 $N=5^2-13\cdot1^2=12$，这里 $x=5$，$y=1$，我们可把 N 写成反形：

$$\begin{aligned} &13(5\cdot5 - 1\cdot18)^2 - (18\cdot5 - 13\cdot1\cdot5)^2 \\ &\quad = 13\cdot7^2 - 25^2 \end{aligned}$$

或

$$\begin{aligned} &13(5\cdot5 + 1\cdot18)^2 - (18\cdot5 + 13\cdot1\cdot5)^2 \\ &\quad = 13\cdot43^2 - 155^2. \end{aligned}$$

当给定数 N 的组成全然不清楚时，即使 D 是一个指定数，究竟把 N 表示为 x^2+Dy^2 还是 x^2-Dy^2，这并不总是一件轻而

易举的事.

若 D 是示性数,而已知 N 为素数,上述判定可利用基于平方剩余原理的规则.数的“线性”形式指出了这一可能性.表 98 中给出了不超过 19,且不含平方数除数的 D 值,两类形式都齐全了.

D	线性形式	二次形式
1	$4K+1$	x^2+y^2
2	$8K+1,3$	x^2+2y^2
3	$6K+1$	x^2+3y^2
5	$20K+1,9$	x^2+5y^2
6	$24K+1,7$	x^2+6y^2
7	$14K+1,9,11$	x^2+7y^2
10	$40K+1,9,11,19$	x^2+10y^2
13	$52K+1,9,17,25,29,49$	x^2+13y^2
15	$30K+1,19$	x^2+15y^2
-1	$4K\pm1$	x^2-y^2
-2	$8K\pm1$	x^2-2y^2
-3	$12K+1$	x^2-3y^2
-5	$10K\pm1$	x^2-5y^2
-6	$24K+1,19$	x^2-6y^2
-7	$28K+1,9,25$	x^2-7y^2
-10	$40K\pm1,9$	x^2-10y^2
-11	$44K+1,5,9,25,37$	x^2-11y^2
-13	$26K+1,3,9$	x^2-13y^2
-14	$56K+1,9,11,25,43,51$	x^2-14y^2
-15	$60K+1,49$	x^2-15y^2
-17	$34K\pm1,9,13,15$	x^2-17y^2
-19	$76K+1,5,9,17,25,45,49,61,73$	x^2-19y^2

[273] **表 98 素数的线性与二次形式**

设我们想测试一下,把素数 151 表为 x^2+7y^2 的可能性,我们可以先用 14 去除它,得出余数 11,从而 151 是 $14K+11$ 形式的数;由上表可知,它肯定可以表示为 x^2+7y^2 的形式.实际情况也确乎如此,因为 $12^2+7\cdot1^2=151$.再来看素数 79,它能否表作 x^2-5y^2 的形式呢?由于 79 是 $10K-1$ 形式的数,因而由表

可知，这是做得到的；实际上 $18^2-5\cdot 7^2=79$ 即是其解答.

*　　　*　　　*

二次形式的理论使人们得以判定：具有给定形式的数的除数有什么可能形式. 例如，我们已经发现，两个互质的平方数之和的任一因子也是两平方数之和. 类似地，$x^2\pm 2y^2$ 以及 $2x^2\pm y^2$ 的除数也具有类似性质. x^2+3y^2 与其反形 $3x^2+y^2$ 的任一奇除数也都是这样，此断言对 x^2-5y^2 与 $5y^2-x^2$ 也成立.

数 18000001 等于 $2(3000)^2+1$；因此它的任何一个素除数也应当具有 $2x^2+y^2$ 的形式或其反形 x^2+2y^2. 表 98 已告诉我们，二次形式为 x^2+2y^2 的素数，其线性形式应为 $8K+1$ 或 $8K+3$. 这样一来，在寻找 18000001 的可能除数时，凡是 $8K+5$ 或 $8K+7$ 的素数即可立即排除. 这样就削减了一半的工作量. 经测试后，此数的两个素除数果然是 $3307=43^2+2\cdot 27^2$ 以及 $5443=49^2+2\cdot 39^2$. 它们都是兼有 $8K+3$ 与 x^2+2y^2 两种形式的数.

*　　　*　　　*

有些自然数可以用几种办法表作同次幂的和. 第 15 章我们已对表示为两个平方数之和的情况作了充分讨论. 但对表示高次幂来说，相应的数学解析远非易事. 能用两种办法表示为两个立方数之和的最小者是

$$1729=1^3+12^3=9^3+10^3.$$

而能用三种办法表示为立方和的数，下面的数 175959000 可能是最小的：

$$175959000=70^3+560^3=198^3+552^3=315^3+525^3.$$

[274]

在小于 100,000 的自然数中，只有 10 个数能用两种办法表为两立方数之和. 而用两种途径表为四次方和的，下面的数也许是最小了：

$$635318657 = 59^4 + 158^4 = 133^4 + 134^4.$$

* * *

在二次形的现代理论中，$ax^2+bxy+cy^2$ 中的系数 a,b,c 是同变量剥离的，它们像是没有躯壳的鬼魂在远离凡夫俗子视野的、数学化的影子世界里踽踽而行，飘过来又荡过去. 不过，我们必须匆忙赶路，前往我们旅程的终点，因为，过分去想那种形态的事情，会把自己的思维搞得七颠八倒.

参考文献

Barlow, P. *Theory of Numbers*. London: J. Johnson & Co., 1811.

Carmichael, R. D. *Theory of Numbers and Diophantine Analysis*. New York: Dover Publications, Inc., 1959.

Cunningham, A. *Quadratic Partitions*. London: F. Hodgson, 1904.

Dickson, L. E. *History of the Theory of Numbers*. 3 vols. New York: Chelsea Publishing Co., 1950.

——. *Introduction to the Theory of Numbers*. New York: Dover Publications, Inc., 1957.

——. *Modern Elementary Theory of Numbers*. Chicago: University of Chicago Press, 1939.

——. *Studies in the Theory of Numbers*. New York: Chelsea Publishing Co., 1962.

Mathews, G. B. *Theory of Numbers*. New York: Chelsea Publishing Co., 1961.

Vinogradov, I. M. *Elements of Number Theory*. New York: Dover Publications, Inc., 1954.

[275]

第24章 石城虎踞

我们即将到达数字王国旅游观光的最后一站.在世上最聪明,计谋多端的数学家也未能攻破的一座石头城前面道声“再会”.伟大的法国学者费马说他已经打开了城墙的缺口,但一些数学家们不以为然.尽管如此,费马的处世为人是少有的正直无欺.凡是他声称他已经证明过的定理没有一个遭到否定.唯一的个别例子也不能成为指责者的口实,在那里,费马相信是正确的事实遭到了后人的否定,即便如此,费马当时也讲得清清楚楚:他并未找到足够的证据.

费马收藏了一本丢番图的数论著作,在书的边缘上做了许多批注.他在有关标题“把一个平方数分成两个平方数之和”的某一页上写下了批注:“反之,不可能把一个立方数,分解成两个立方数,也不能把一个四次方数分解成两个四次方数.一般地说,除了二次方以外,不可能把一个乘幂分解成两个同次幂之和.对此,我已找到了一个奇妙的证法.不过,页边地位狭窄,容纳不下.”后人多么希望,巴舍(Bachet)所译的这部丢番图著作边页能够加宽一些,或者费马的话说得更加“开门见山”一些,不要如此遮遮掩掩.

费马的话意思很清楚,n 大于 2 时,$x^n+y^n=z^n$ 是没有整数或有理数解的.他曾经打算写一本书,讲一讲解决数论问题的独特方法,但对任何人都不肯稍稍宽限的死神来把他叫去了.费马何以能得出这一结论?后人找不到片言只语,蛛丝马迹.不管后

来者们如何坚持不懈，孜孜以求，问题却是始终解决不了. 方程 $x^n+y^n=z^n$ 称为费马的“最后定理”(大定理)，既不是因为它冒出头来却又寂无下文，也不是费马所发表的最后一个定理，而是在他提出来的众多定理中，最后一个无法证明也不能否定的命题.

费马为人诚实，名声极好，因而确实有人深信他有过一个证[276]法. 费马生平只有一次谬误，他曾认为 $2^{2^x}+1$ 恒能得出素数，但对许多 x 值来说，“费马数”却是合数(见第 17 章). 但即便是这些例外情况也只能加强他的“诚实”信誉，因为费马曾公开宣布他未能找到一个证法来支持他的信念.

不过，信誉终究未能代替证明，即便像费马这样的“完人”也不行. 一代又一代的数学家们都曾企图证明或推翻他的定理. 就像是千方百计地寻找西北航道[1]那样，这些男男女女虽然劳而无功，却在数学王国里发现了许多丰硕成果，也积累了大量信息财富. 如果定理很容易证明的话，那就不可能得到这些收获. 企图证明费马大定理，作为这个尝试的一个直接后果是：库默发现了名符其实的一个数的新大陆.

困难究竟在哪里呢？我们在第 14 章里已讲过，怎样去求方程 $x^2+y^2=z^2$ 的解，要多少有多少. 但为什么 $x^3+y^3=z^3$ 或 $x^4+y^4=z^4$ 就没有解？想写出两个立方数，使其和等于另外两个立方数，几乎没有什么特别困难，譬如说，$12^3+1^3=10^3+9^3$. 但在高度和谐的数学世界里，如果真有可能使 $x^n+y^n=z^n$(或其变相形式：$x^n+y^n+z^n=0$，这里，n 与 x、y、z 互质)，那肯定与整数的某种微妙本质是根本抵触的，那将不合逻辑，模式的漏洞也无法弥合.

从毫不涉及的领域发起进攻，研究家们已经证明，上述不定

[1] 西北航道(North-West Passage)是指：从大西洋经欧、亚两洲北部诸海到达太平洋的航道. ——译者注.

方程或其变相形式对小于 100 的 n 都是无解的. 起先, 对 37, 59 与 67 还有所怀疑, 后来确证这些数也不可能; 接着, 又把上限相继扩展到了 7000; 14000; 8332403; 253747889. 对 $n=2^{3217}-1$, (这是一个素数), 也是不可能有解的. 不管采用什么手段, 结论总是相同——方程无有理数解. 除了一些能满足极为复杂的先决条件者之外, 大定理对 n 的几乎一切整数值都成立. 但由于无穷大王国辖境如此之广, 定理终究不能认为已得到了彻底的证明, 除非一切例外情况都被排除, 对 n 的一切值统统都成立. W·W·R·鲍尔说过: "只是数值验证价值不大; 无人怀疑定理的真实性, 但主要的着眼点在于这样一个事实, 即我们尚未能够得出定理的一个严格证明."

如果从 $z^n-y^n=x^n$ 出发, 并分解因子, 则有

$$(z^{\frac{n}{2}}+y^{\frac{n}{2}})(z^{\frac{n}{2}}-y^{\frac{n}{2}})=x^n.$$ [277]

x, y, z 当然可视为互质, 因若它们有公因子的话, 事先就可以约去. 另外, n 也可看作与 x, y, z 互质. 其次, 若括弧里的两个表达式有公因子的话, 则它们的和 $2z^{\frac{n}{2}}$ 也应如此. 但由于 z 与 y 互质, 括弧里的两个表达式唯一的公因子只能是 2. 又因它们的乘积是一个完整的 n 次幂, 我们必有下列两者之一, 即

$$z^{\frac{n}{2}}+y^{\frac{n}{2}}=2^{n-1}p^n \text{ 与 } z^{\frac{n}{2}}-y^{\frac{n}{2}}=2q^n$$

或

$$z^{\frac{n}{2}}+y^{\frac{n}{2}}=2p^n \text{ 与 } z^{\frac{n}{2}}-y^{\frac{n}{2}}=2^{n-1}q^n,$$

因为只有这样才能使其乘积 $2^np^nq^n$ 是一个完全的 n 次幂. 不论哪种情况都将有 $x=2pq$. 通过加减法可求出 z 与 y, 前一种情况有

$$z^{\frac{n}{2}}=2^{n-2}p^n+q^n, \quad y^{\frac{n}{2}}=2^{n-2}p^n-q^n,$$

后一种情况则有

$$z^{\frac{n}{2}} = p^n + 2^{n-2}q^n, \quad y^{\frac{n}{2}} = p^n - 2^{n-2}q^n.$$

但不论是

$$z = (2^{n-2}p^n + q^n)^{\frac{2}{n}}, \quad y = (2^{n-2}p^n - q^n)^{\frac{2}{n}}$$

还是

$$z = (p^n + 2^{n-2}q^n)^{\frac{2}{n}}, \quad y = (p^n - 2^{n-2}q^n)^{\frac{2}{n}}$$

全都桀骜不驯，无法驾御，因此，n 大于 2 时，既不能发现整数或分数解，也不能证明求解不可能.

*　　　*　　　*

在我们试图对一般情形发起另一次进攻之前，让我们先考虑一些基本事实，并用来证明 $x^4+y^4=z^4$ 的不可能性——这个证明比较简便，还可以顺便讲一讲费马的无限递降法. 如果两个整数互质而且它们的乘积为平方数，则稍为考虑一下即可肯定这两个数都必须是平方数. 因为，整数 N 作为平方数的显著特征是：当 N 表示为质因数的连乘积时，每个素数的幂指数都必须是偶数，即：

$$N = p_1^{2a_1} \cdot p_2^{2a_2} \cdot p_3^{2a_3} \cdot \cdots \cdot p_n^{2a_n}.$$

[278] 例如，在表示为质因数及其幂的连乘积时，1936 等于 $2^4 \cdot 11^2$，由于两个指数都是偶数，所以此数是个平方数. 但 $1940=2^2 \cdot 5 \cdot 97$，由于 5 与 97 的指数是奇数 1，所以 1940 不是平方数.

如果两整数互质，则它们不可能具有公共素因子，因而，若其乘积是平方数，则组成平方数的素数的偶指数必将出现在两个因子里. 换言之，这两个因子本身都应该是平方数. 显然，上述事实对两两互质，有着许多因子的质数也成立，所以，如果其乘积是一个平方数，则每个因子也必定是平方数.

类似地可推得，若两个互质整数之乘积是一个 n 次方幂，则每个数都应是个 n 次方幂. 现在考虑 $x^4+y^4=z^4$ 这一特款，这里

的三个变量都可看成互质——因若其中的任两个数具有公因子，则第三个也必然具有公因子，从而可以事先约去. 下一个事实是：若$(x^2)^2+(y^2)^2=z^2$不可能有解，则$(x^2)^2+(y^2)^2=z^4$也不可能有解. 由第14章所讲过的毕氏三角形的法则，前者可以表达为$x^2=m^2-n^2$，$y^2=2mn$，$z=m^2+n^2$. 这里，m，n必须互质，否则x，y，z就不会互质；另外，m，n应具有不同奇偶性——一奇一偶——否则m^2-n^2与m^2+n^2就将都是偶数，而x，y，z势必至少具有一个公因子2，这就违反了它们都是互质数的假定. 从$x^2=m^2-n^2$中又可看出不可能是m偶n奇，这是由于m显然为本原毕氏三角形的斜边，而在这种三角形中，必然有一条直角边恒为偶数，而斜边恒为奇数. 由此可知只可能是n偶m奇(请参看第14章的公式1). 于是，在表达式$x^2=m^2-n^2$中，我们必须令$n=2pq$，$m=p^2+q^2$，$x=p^2-q^2$，这是再次应用了毕氏三角形法则而得的结果. 接着，由于$y^2=2mn$，这也相当于$2(p^2+q^2)(2pq)=4pq(p^2+q^2)$. p，q也应互质，由于$4pq(p^2+q^2)$是个平方数y^2，由此即可判明p，q，p^2+q^2都应该是平方数. 于是，可设$p=r^2$，$q=s^2$，$p^2+q^2=t^2$. 把p，q值代入最后一式，即有$r^4+s^4=t^2$. 又因$x=p^2-q^2$，于是有$x=r^4-s^4$. 由$y^2=4pq(p^2+q^2)=4r^2s^2t^2$，便得$y=2rst$. 另外，$z=m^2+n^2=(p^2+q^2)^2+(2pq)^2=(r^4+s^4)^2+(2r^2s^2)^2=t^4+4r^4s^4$. 既然$z=t^4+4r^4s^4$，可知$z$应大于$t^4$，或者说，$t$应小于$z^{\frac{1}{4}}$.

现在，无限递降法要出台了. 我们发现，方程$r^4+s^4=t^2$的形状同$x^4+y^4=z^2$的形式一模一样，可是t小于$z^{\frac{1}{4}}$. 因此，如果后一方程有解(0解不能算数)，则必然有另一个更小的整数解 [279] (因为t小于z). 类似地，若$r^4+s^4=t^2$真的有解，则必将存在另一个解，其中t_1应小于$t^{\frac{1}{4}}$. 这样的论证可以继续无限多次. 但这显然是荒谬可笑的，因为z原本是一个有限的正整数，人们决不可能找到越来越小的正整数来满足同一形式的方程. 于是，x^4+

$y^4 = z^4$ 必定无解.

某些研究者想利用费马无限递降法的表面上讲得通的修正形式来解决大定理的证明问题. 他们不从一个立足点开始,由此"递降"到明显的矛盾,而代之以另一种论证形式:如果某种解法依赖于较大或较小的解,那么它就不可能存在. 方程形成了一种无法穿透的循环论证. 有一位作者不想使用无限递降或无限递升的说法,而称之为递归式证法. 他说得过于简单,很有点教训人的格言式味道:"当我们对一方程(或方程组)有了一个完全解,而它却不能产生某种形式的解时,那么这种形式的解就不存在. 在我们获得这样一个解之前,它首先要求我们得有这样一个解,而不论所求解是不是小于、等于或大于应有之解. 但这是做不到的."①

对 $x^4+y^4=z^4$ 的证法不能适用于 $x^3+y^3=z^3$,不可能性的证明要困难得多. 早在费马之前七百多年,阿拉伯人已知其不可能成立,他们甚至还给出过一个证法,不过,那个证法是错的.

*　　*　　*

就一般情况而言,只需对素数指数p给出证明就够了,因对任何合数指数$n=mp$(p是一个素因子),都必然有$(x^m)^p+(y^m)^p=(z^m)^p$. 若对任何整数 X,Y,Z 及素数 p,方程 $X^p+Y^p=Z^p$ 不能成立,则当 $X、Y、Z$ 为乘幂时,方程也不能成立. 当 n 是 4 的倍数时,方程显然不能成立,因为我们已知 $n=4$ 时它不能成立.

现在让我们重温一下因式分解的若干初等原理. 表达式 x^2+y^2 是不能分解的,这意味着它不能分解为"实"线性因式. 如 [280] 果我们坚持要线性因子,那就必须引入虚数 $i=\sqrt{-1}$. 于是有 $x^2+y^2=(x+iy)(x-iy)$. 你们可以回忆得起 $i^2=\sqrt{-1}\cdot\sqrt{-1}$

① 参阅沃尔什(C. M. Walsh),"通过一种新方法,试图证明费马大定理",纽约,G・E・斯德克公司,1932 年出版. —— 原注.

不知所云,纯属胡说八道. —— 译者注.

$=-1$，于是$(x+iy)(x-iy)$等于$x^2-i^2y^2=x^2+y^2$. 如果我们想分解x^p+y^p（这里p是一个奇数，其特例是一个奇素数），便可得出

$$x^p+y^p=(x+y)(x^{p-1}-x^{p-2}y+x^{p-3}y^2-x^{p-4}y^3+\cdots-xy^{p-2}+y^{p-1}).$$

例如，

$$x^7+y^7=(x+y)(x^6-x^5y+x^4y^2-x^3y^3+x^2y^4-xy^5+y^6).$$

括弧里头的那个长长的表达式是一个“代数素因子”，也就是说，没有办法把它进一步分解成两个或更多个较低次的表达式的乘积. 如果我们仍然坚持要把结果分解成线性因子，那就不得不再次引入虚数i，但这一次就不像分解x^2+y^2时出现的简单形式了.

需要有点耐心来解释一下稍为难一点的概念. 每一个数x有两个平方根，$+\sqrt{x}$与$-\sqrt{x}$. 每个数有三个立方根，其中之一为实数根，两个是复数根. 例如，1 的三个立方根是$(-1+i\sqrt{3})/2$，$(-1-i\sqrt{3})/2$，1. 这三个数中的任一个，立方后都等于$+1$. 如为了方便，我们用“a”来代表$(-1+i\sqrt{3})/2$，则a^2就代表$(-1-i\sqrt{3})/2$，它是第二个“1 的复立方根”，而a^3就是简简单单的$+1$. 与此类似，1 的n个复根也都可以表为它的第一个复根的整数乘幂.

我们坚持要把$x^{p-1}-x^{p-2}y+x^{p-3}y^2-x^{p-4}y^3+\cdots-xy^{p-2}+y^{p-1}$分解为线性因子，就势必要将 1 的$p$次复根引入话题. 方程$x^p+y^p=z^p$于是变成了下列形状

$$(x+y)(x+ay)(x+a^2y)(x+a^3y)\cdots(x+a^{p-1}y)=z^p,$$

这里a的每一个幂代表了 1 的某个p次复根. 这些线性因子是

彼此互质的，由于其乘积为 z^p，人们据此认为，每一个都是完整的 p 次幂. 对实数来说，这无疑是正确的. 那么，对于含有淘气小鬼 i 的复数，它也对吗？

一旦我们对此提出疑问，这简直像是在怀疑我们自己是否神志清醒了. 用纸牌搭建起来的我们的数学房子似乎要倒坍下来，远远地恍惚可以听到柴郡猫[①]的傻笑在逐渐消逝，这一切与化作轻烟散失的费马的幽灵又是多么惊人地类似！整个数论建[281]立在"唯一分解定理"的基础之上，即一数能有一种且仅有一种方法分解为素数幂的连乘积. 尽管在实数王国中这是千真万确的事实，但整数的这一基本性质尚可推广引申，使它在任何数字王国中未必都能成立.

设想我们的数字王国只包含 $4x+1$ 形式的整数：1，5，9，13，17，21，25，29，33 等等. 任何其他形式的整数都不属于我们这个"梁山泊"；我们只生活在 $4x+1$ 的世界里. 在这个独立王国里，只有 1 与本身是因子的 9 算不算一个素数呢？"你不考虑 $3\cdot 3$ 吗？"也许你要提出疑问. 但是，在这个新王国里，是没有 3 这种整数的. 数 21 也应视为素数，可是，25 却是一个合数，而且还是一个平方数，因为 5 与 5^2 都是王国的子民. 数 49 亦应视为素数，因为 7 是化外之民.

现在我们将得到一些惊人的结果. 两个"素数"9 与 49 的乘积是 $441=21^2$，这里，441 与 21 都属于新系统. 于是，我们得到一个非常怪异的结论：两个素数（当然也是"互质"的）的乘积竟是一个平方数！ 在此新数系中，9，21，33，77 全是素数. 但 $693=9\cdot 77=21\cdot 33$，因此 693 居然可以用两种不同方式表为素数幂的乘积（这里的乘幂都指一次方）.

在通常的算术里，如果一个整数能整除另外两个整数的乘

---

① 柴郡猫是著名儿童文学作家刘易士·卡洛尔笔下的童话人物，它经常无缘无故地露齿傻笑，其故事详见《爱丽丝漫游奇境记》. ——译者注.

积，但不能整除其中的任一个，则此整数不可能是个素数，但在这里，693 能被 21 整除，而 9 与 77 不行，然而 21 还是一个素数.

在引进“超越数”$4x-1$ 以后，$4x+1$ 王国中的种种怪异情况便能得到纠正. 一切都恢复到正常状态，仍然是莺歌燕舞，鸟声啁啾.

数学家总是喜欢使用类比推理，而不管是否导致荒诞结论. 如果我们不局限于生活在实数行星上，而允许前往 $3+2\sqrt{-1}$（一般情况为 $a+bi$，这里 i 仍然表示 -1 的平方根，而 a，b 为整数）的世界里旅游观光一番，那么我们会发现什么样的新奇数学土著呢？在那里，唯一分解定理还成立吗？

我们从这样一个新奇概念出发：i 或 $\sqrt{-1}$是“复数行星”上的一个“单位”，因为它能整除任何一个形为$a+bi$的数. 例如$3+2\sqrt{-1}$或$3+2i$除以i后就变成了$-3i+2$.（读者们当能回想得起以前从代数课本里学到过的知识：$i^2=-1$，$i^3=-i$，$i^4=1$.）类似地，5 也能被“单位”整除，得出商 $-5i$. 在这个王国里共有四个“单位”：±1 与 $\pm i$. 如果一个整数不具有 $a\pm bi$ 形式的因子（这里 a，b 是通常的整数），那就定义为素数，而当它具有此种形式的因子时，它应算作合数. 例如： [282]

$$5=(2+i)(2-i)=4-i^2=4-(-1)=4+1,$$
$$13=(3+2i)(3-2i)=9-4i^2=9-(-4)=9+4,$$
$$17=(4+i)(4-i)，等等.$$

于是 5，13，17 都是合数. 由于$(a+bi)(a-bi)=a^2+b^2$，而所有 $4x+1$ 形状的素数都能表示为两个平方数之和，因而在这个复数行星上，一切通常认作素数的 $4x+1$ 形式的数在“新观点”下都是合数. 在此数域中，唯一的实素数是 $4x-1$ 形式的普通素数，例如 3，7，11，19 等等. 合数 5，13，17，…的除数 $2\pm i$，$3\pm 2i$，$4\pm i$，$a\pm bi$ 等则也称为“素数”. 最后，数 $1-i$ 既不是实数，又不

是 $4x+1$ 形的素数，它也应看作素数. 此外，数 2 占有一席特殊位置，它被看作一个平方数，因为它等于 $i(1-i)^2$，而后者是一个平方数与一个“单位”的乘积.

有时候，像实数的整数一样，代数数中的形为 $a+bi$ 的合数只能以唯一方式表示为素数幂的乘积. 例如，$-23+41i=(1+i)(2+i)(3+2i)(4+i)$. 所有这些因子都不再具有同型除数①，因而它们都是素数. 而其他素数的乘积也不可能等于 $-23+41i$. 此种情况，在 $a+b\sqrt{3}i$ 这样的代数数王国里也是正确的. 或许人们将会仓促地下结论，在所有的数域里因式分解的唯一性都能成立，然而事实并非如此.

我们发现，在 $a+b\sqrt{-5}$ 的复数行星里，像 21 这样的数，竟然有三种不同方式表成为该数域中“素数”幂的乘积，即 $3\cdot 7$，或 $(4+i\sqrt{5})(4-i\sqrt{5})$，或 $(1+2i\sqrt{5})(1-2i\sqrt{5})$. 所有这些数都是“素数”，除了数域中的“单位”以外，其他整数都不能将[283]它们整除.

还有，$2+i\sqrt{5}$ 与 $2-i\sqrt{5}$ 的乘积是 9，一个平方数，然而两个因子都是“素数”，因它们都不是数域中两个非“单元”整数之积. 这不是造成混乱吗？也许真的如此. 在数学家们发现一个“代数数整数”可用几种不同办法分解为素数幂的连乘积时，他们不免失态，简直有点乐极忘形起来. 他们的感受很有点类似于一些近代物理学家，把一切事物都归结到一个数学方程. 当然，庄稼汉依旧像平时一样，拖着沉重的脚步荷锄回家，不会去考虑这种牵强附会、进退维谷的两难处境. 可是，农民们照样身心健全地

---

① 为了证明这一点，可假定 $3+2i$ 这样的数是两个因子 $a+bi$ 与 $c+di$ 的乘积. 于是，乘积为 $(ac-bd)+i(ad+bc)$，由实部与虚部分别列出等式，可得 $ac-bd=3$，$ad+bc=2$. 但没有任何正、负整数解满足这两个方程. 从而说明 $3+2i$ 是一个素数. ——原注.

活着，所以，这种东西毕竟无关宏旨.

不过，在数学世界里毕竟要把事情梳理得井然有序，而库默这位奇才毅然担当了这件事情. 他的推理如下：如果说，在实整数行星中由于引进了 $4x-1$ 形式的数，作为狭隘的 $4x+1$ 数域的补充，从而恢复了因式分解的唯一性；那么，在复数行星中，能不能也来引进一些什么数，使因式分解的唯一性得以重新确立呢？于是，他发明了一族"理想数"，从而结束了无政府的混乱状态，恢复了以往的安静局面. 在 $a+b\sqrt{-5}$ 的数域中，如果 T^2 等于 $c+d\sqrt{-5}$ 或 $c-d\sqrt{-5}$，则 T 叫做"理想数"，或者简称"理想"①，由此可见 $T=\sqrt{c\pm d\sqrt{-5}}$. 此处，c，d 必须是整数，并允许它们有公因子，该公因子可以是一个平方数或一平方数的5倍.

这个数域共分四类，其中有着我们通常称之为"素数"的数. 第一类包括通常的素数，例如

$$29=(3+2i\sqrt{5})(3-2i\sqrt{5}),$$
$$41=(6+i\sqrt{5})(6-i\sqrt{5}),$$
$$61=(4+3i\sqrt{5})(4-3i\sqrt{5}),$$

其中的每个数都可表为 a^2+5b^2 形式. 但是，这种数在 $a+b\sqrt{-5}$ 这个"王国"里是视为合数的.

第二类中的数有 3，7，23，…，它们不能表示为 a^2+5b^2 的形式，然而它们的平方却可以做得到：

$$3^2=(2+i\sqrt{5})(2-i\sqrt{5}),$$
$$7^2=(2+3i\sqrt{5})(2-3i\sqrt{5}),$$
$$23^2=(22+3i\sqrt{5})(22-3i\sqrt{5}).$$

[284]

① 本段可参看我国数学界元老的权威著作《吴文俊文集》第 108—109 页，山东教育出版社，1986 年第一版. —— 译者注.

第三类数有 2，11，13，17，…，不论这些数本身或其平方均不能表示为 a^2+5b^2 的形式. 这些数，在我们的普通数域以及 $a+b\sqrt{-5}$ 数域中都是被看作素数的.

第四类中只有一个数 5，它自成一类. 这是一个"平方数"，因为 $5=(\sqrt{-5})^2\cdot(-1)$，而 -1 是数域中的单位数.

第二类中的数显然是理想数的乘积，例如，$3^2=(2+i\sqrt{5})(2-i\sqrt{5})$，而 $\sqrt{2+i\sqrt{5}}$ 与 $\sqrt{2-i\sqrt{5}}$ 都是理想数，可记为 T_1，T_2，我们有：

$$3^2=\left(\sqrt{2+i\sqrt{5}}\right)^2\left(\sqrt{2-i\sqrt{5}}\right)^2=T_1^2\cdot T_2^2$$

$$\text{或 } 3=T_1\cdot T_2.$$

理想数是一种代数数，它们可以通过加法与乘法来自我繁殖，从而形成了很独特的一类数. 我们这里不想占用多少时间去谈论它们的哪怕是为数寥寥的一些特异性质.

Z·E·狄克逊对库默的大脑里培育出来的婴儿说了这样一些话："机关是如此之微妙，甚至一位专家也必须小心翼翼地进行操作，目前，相对于更简洁，更一般的戴德金的理论而言，这种数只是具有历史意义而已. "大部分人赞同大名鼎鼎的德国数学家李奥波特·克朗尼克(Leopold Kronecker)的看法，很厌恶理想数与一般"代数数"这类不自然的"人造事物". 许多人对克氏的说法持有同感："上帝创造了整数，其他都是人造的. "读者们至少要学会小心谨慎，不要在唯一的因式分解问题上匆忙地作出结论，也要防止重犯一些难以避免的错误，对企图证明费马大定理的专业人员或业余爱好者，它简直像是一个害人不浅的罗勒莱. [①]

① 根据德国民间传说，罗勒莱是经常出没于莱茵河岩石上，凭其美貌与歌唱引诱船夫而使船只触礁沉没、船员葬身鱼腹的女妖精. ——译者注.

* * *

不论用什么手段,渊博的或是初等的,也不论用什么论证,简单的或是精巧的,费马大定理的每一个所谓的证法中都存在着严重瑕疵.于是在1823年,继而又在1850年,巴黎的科学院都公开宣布要给完善的证法提供一笔重奖.这就为数以千计的数学冒险家与不学无术之徒大开方便之门.尖酸刻薄的奥古斯都·德·摩根(Augustus de Morgan)在其著作《悖论汇编》中不留情面地彻底揭露了一批白痴与愚昧无知的骗子.

1857年法国科学院授予理想数的发明者E·E·库默一枚价值3000法郎的金质勋章,以表彰他在复数领域中的卓越研究,然而他并不是原先意义上的奖金得主.尽管如此,他之得此重奖乃属理所当然.正是由于他的研究使人们可以立即排除指数n小于100时,方程$x^n+y^n=z^n$成立的可能性(除了$n=37$,59,67之外,而这几个数又被其他办法迅速了结).布鲁塞尔科学院在1883年也设置了一笔奖金,可是,在审读了所有的来稿以后,却下发了一个反对的结论性报告. [285]

1908年,德国达姆斯塔特地方的F·P·服尔夫斯凯尔博士(Dr. F. P. Wolfskehl)赠给哥庭根皇家学会十万马克的巨款,以奖励给出费马大定理的完善证明者."这笔奖金的存在引来了一大批虚假证明.一些没有受过专业训练的人也妄想进攻这个难题,这种人越来越多,"R·D·卡米凯尔深感遗憾地说.在1908至1911年这段时间,提交的错误证明超过一千篇.托比亚斯·但捷格说道:"从那个时候以来,把许多无谓精力浪费在化圆为方、任意角的三等分、永动机等问题上面的业余研究家们开始转向,集中在费马大定理的证明上……幸而公告规定来稿必须是印刷品,这或许是给许多狂热者泼了一盆冷水……几乎所有的来稿都具有这样一些特点:作者们完全无视在这个问题上已经完成的大量成绩,他们也根本不想去了解问题的难点和症结究竟在哪里."

绝大多数解法都是由作者们自费印刷的，几乎没有一家有自尊心的出版商甘愿冒声名扫地的风险去印刷那种提交上来的昏庸愚昧的“杰作”. 许多投稿者根本没有本事去掌握最初步的库默的理想数原理. 这倒并不意味着只有通过理想数才能获得问题的解. 但这种方法要比任何其他方法更能击中问题的要害.

声称已经解开了戈尔地雅斯王的难解之结①，将成为数学王国主宰的人，他们到底有点什么能耐呢？这可从下面一段奇文里略窥一豹，此文引自 1914 年波士顿所印行的一本小册子，作者名叫 G・W・皮尔士(Pierce)，书名叫做《比费马更伟大的定理被我证明了》.

作者从其光辉的观察开始：$1^1+2^1=3^1$；$6^{-1}+3^{-1}=2^{-1}$. 然后他冗长而自命渊博地宣布 $12^3+1^3=10^3+9^3$，似乎这是非常独特而新奇的东西. 当然这种立方数对还有好多，例如：$9^3+15^3=2^3+16^3$；$15^3+33^3=2^3+34^3$；$16^3+33^3=9^3+34^3$；$19^3+24^3=10^3+27^3$；$50^3+29^3=8^3+53^3$. 甚至还有三对立方数能等和的例子：$560^3+70^3=552^3+198^3=525^3+315^3$. 另有一些得自一般公式的无限多组解. 看来这位作者很有造化，他并不了解它们的关系. 这篇高深论文的价值，可从其结尾的一些奇谈怪论中大体地评估出来：

[286]

> 我在梦里见到一个“约翰牛”(英国佬)，不算太胖，其人名叫“威克菲”，身材魁伟，面目黧黑，一本正经，我在入睡前曾经进见过他.(那是为了有利可图的工作，为了比利时人的利益，是这样的吗？)星期天早晨(1914 年 6 月 12 日)在煤气灯光下我开始执笔，我发现了对

① 戈尔地雅斯的结来自希腊神话，戈尔地雅斯是费吕加国王. 按照神谕，能解开此结者即可为全世界的统治者. 后来，此结被马其顿国王亚历山大大帝用刀劈开，也算是解决了. —— 译者注.

我说来是全然新奇的事情(除了 $n=3$ 以外,对一切正整数,或许还有负整数?今天是1914年8月12日——多年以前纯属偶然地发现并证明了),无疑来自费马本人的传授?每一次测试都通过了(其中可能有一些错误,不是上帝的,而是我自己造成的,但都已改正了),现在是天黑以前的下午8点钟,我坚决相信:许多算术级数的 n 次幂(大于2的奇数)之和,除以它们的一次方之和时,将是一个整数!?我以为(反来复去,现在,过去,将来,手写或通过印刷品)这是一种大脑与心灵现象.我的母亲是位心灵学者,女预言家,她对我说:"乔治,你可永远成不了一个诗人."还有我的父亲,我的心灵与肉体都是从他那里继承过来的,还有我的老兄(比我大2岁,父母的第一个孩子),他不是一个天生的凯撒大帝,还有我的小弟弟(父母的第五个孩子,是老小),是一个骄傲而甜蜜的小把戏,超自然的聪明,他比我要小14岁,在我不在场时他会叫我"我们的乔治",他不幸在6岁时得了浮肿毛病,我怀疑是他在助我一臂之力.为了他们在天堂里谋到一个永久职位(有些人担心他们也许谋不到这份好差使),我要把算术、代数贡献出来,作为我送给各位的一个礼盒.

乔治·温斯洛·皮尔士,
哈佛学院文学学士,1864年
哈佛学院文学硕士,1867年
P·P·(标点学教授)
波士顿周刊(1)
康古德西大街126号,
美国马萨诸塞州波士顿市.

我是《一位代数学家的毕生罗曼史》的作者,此书曾于1891年在波士顿市出版,并作为礼品经由美国国家博

物馆散发到一百个国家的图书馆.

(波士顿市老角落书店有售,作者自办发行,需要购书者可汇款给作者.)

祝大家圣诞节快乐,作者愿意免费赠送100本给真正的朋友.

* * *

近年来,为金钱卖力工作以及头脑不太健全的人难免要感到失望.第一次世界大战以后爆发的德国通货膨胀,使十万马克奖金不值一美分的若干分之一.即使这些人真正发现了[287]天上的虹彩,他们在破罐子里拿到的也只有可怜巴巴的一点东西."死后的证明与新闻发布会将在德国数学物理的成就的演说大厅里进行."当然仍有一些谨慎与严肃的研究者还在不断地埋头工作,本世纪内人们终将看到问题的完全解决,这不算是太轻率的预言吧.[①] 荣誉纪念堂将为证明者(他或她)留出神龛.

一位不屈不挠的无畏研究者A·维弗利希(Wieferich)在历史上留下铭记,他在最近把指数的下限推进到了百万数量级,对小于这个下限的指数,方程都是无解的.他发现,若p为素数[②],则方程$x^p+y^p+z^p=0$不可能有整数解,除非$2^{p-1}-1\equiv 0 \bmod p^2$,这就一举排除了1093以下的$p$值,因为$p=1093$是

① 此事果真被本书作者说中了.1993年7月1日《科技日报》报道,英国数学家怀尔斯已于1993年6月24日在剑桥大学的学术报告会上证明了费马大定理.《人民日报》几天后也刊登了消息.其后,作者又对自己的证明作了修正,得到世界数学界的肯定.1995年5月,世界权威性学术刊物《数学年刊》(Annals of Mathematics)在第141卷第3期上,以整期的庞大篇幅,发表了怀尔斯先生的修正证明,被称为本世纪最伟大的数学成就之一.

有兴趣的读者可参看《科学》杂志第48卷第3期(1996年第3期,该杂志为双月刊)"费马大定理终于获得证明"一文.——译者注.

② 且如xyz不是p的倍数.——原注.

最小的素数，其平方能整除 $2^{p-1}-1$（见第 6 章）. 由于他的这一发现，维弗利希从服尔夫斯凯尔基金的利息中拿到了 100 马克. 沿着这条路子很快又上来了一个米利马诺夫(Mirimanoff)，他证明了 $3^{p-1}-1$ 也能被 p^2 整除，接着，凡迪佛(Vandiver)在 1914 年证明：$5^{p-1}-1$ 必然也能被整除. 后来，弗洛本尼乌斯(Frobenius)对底为 11 与 17 也得出了同样的结论. 他还证明，若费马大定理成立的话，而 p 是 $6x-1$ 形式的素数，则 $7^{p-1}-1$；$13^{p-1}-1$；$19^{p-1}-1$ 必然都能被 p^2 整除. 在这样一些限制之下，素数指数 p 在不断抬高，到了 1941 年有人证明：如果 $x^p+y^p+z^p=0$，且 x,y,z 没有一个是 p 的倍数，则 p 肯定不小于 253747889. 最近又有人证明：$p=2^{3217}-1$ 也不能满足方程.

* * *

不仅是没有受过专业训练的业余爱好者，即便对知识渊博的大学者，费马大定理也是一块诱饵. 许多人都想来插上一手，但当他们决心放弃它之前已经烧坏了手指. 用英文写出第一本数论书，许多美国数论爱好者对他怀有深厚谢意的彼得·巴罗在一个相当不错的证明的开端就极其丢脸地输得一败涂地. 他从一个似是而非的假定出发：如果你把一些最简分数相加起来，如果任一分母含有一个不含于其他分母的因子，则这些分数之和不可能是个整数. 然而

$$\frac{1}{2}+\frac{5}{3}+\frac{5}{6}=3,$$

[288]

尽管 2 不含于 3 中，6 也不在 2 或 3 中. 此外，还有

$$\frac{7}{2\cdot 3}+\frac{8}{3\cdot 5}+\frac{3}{2\cdot 5}=2,$$

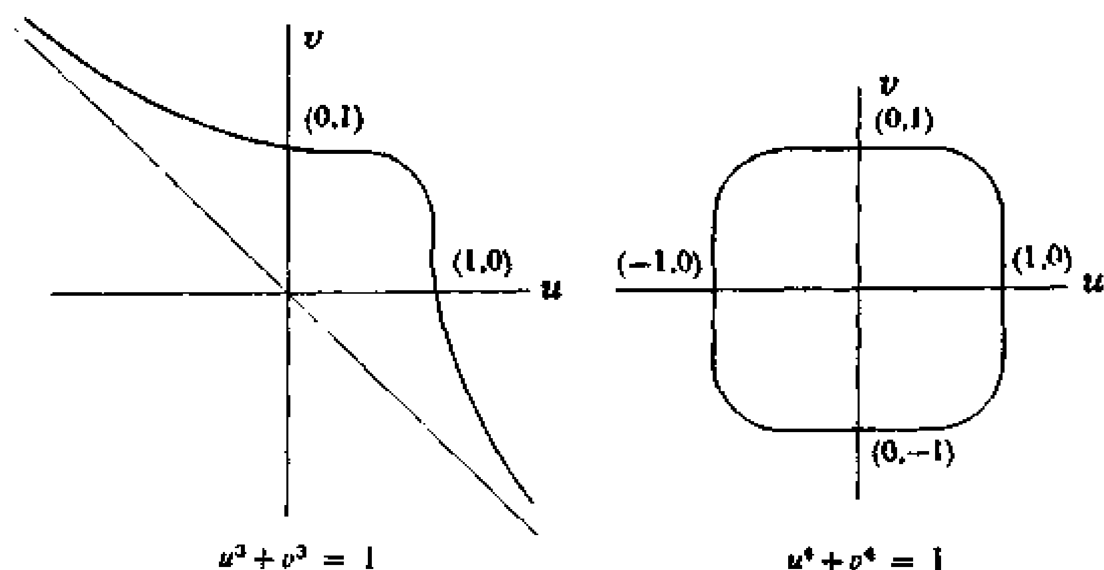
甚至尚有极其明显的反例

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{6}=1.$$

由于证明 π 的超越性而对不可救药的化圆为方问题给以慈悲的最后一击的林德曼(Lindemann)也误入陷阱，他因给出了一个错误证明而使其获奖盾形纹章黯然失色. 企图支撑薄弱环节，这种努力只能把事情弄得更糟. 库默先是认为，完善的证明应立足于这样的事实，即 x^p+y^p 应能唯一地分解为实或复的线性因子，后来他终于意识到这一工作的极度困难. 他发现，原来的想法不能成立，这可能就是他创造理想数域的有力刺激. 后来，他能指出其他备受尊重的数学家们的类似错误. 在这方面，伟大的高斯倒是老谋深算的，他不愿参加比武、远远地躲开了这个妖怪. 他的感觉是，费马大定理仅仅是更广泛的领域中的一个特殊例子而已.

*　　　*　　　*

如果我们在 $x^n+y^n=z^n$ 的两边同时除以 z^n，则可得出 $\left(\frac{x}{z}\right)^n+\left(\frac{y}{z}\right)^n=1$，也可简洁地记为 $u^n+v^n=1$. 图 24 中的开口与封闭曲线分别为最后这个方程在 $n=3$ 与 $n=4$ 时的图象.



[289]

图 24　$n=3,4$ 时，$u^n+v^n=1$ 的图象

n 为更大的奇数或偶数值时，所得出的曲线在性质上也与此类似. 如果费马大定理真能成立的话，则意味着这些曲线具有一种特性：除了它们与坐标轴的交点之外，曲线上的其他点，其坐标不可能是有理数.

* * *

我们已经提到过两个立方和相等的事实，例如：$1^3+12^3=9^3+10^3$. 更一般的关系式 $x^3+y^3+z^3=t^3$ 同样也有无限多组解，其中最简单的情况有：

$$3^3+4^3+5^3=6^3 \quad 和 \quad 1^3+6^3+8^3=9^3.$$

有一个相当复杂的公式来表示这种方程的所有解，不过，就某种类型而言，公式又是相当简单的，不妨在这里讲一讲. 这就是下列恒等式：

$$a^3(a^3+b^3)^3=b^3(a^3+b^3)^3+a^3(a^3-2b^3)^3+b^3(2a^3-b^3)^3.$$

当 $a=2$，$b=1$ 时，此式给出 $18^3=9^3+12^3+15^3$，经化简后，即相当于 $6^3=3^3+4^3+5^3$. 当 $a=3$，$b=1$ 时，我们可得出 $84^3=28^3+53^3+75^3$，而当 $a=3$，$b=2$ 时有 $105^3=33^3+70^3+92^3$.

另一恒等式是：

$$a^3(a^3+2b^3)^3=a^3(a^3-b^3)^3+b^3(a^3-b^3)^3+b^3(2a^3+b^3)^3.$$

这时，对 $a=2$，$b=1$ 可得出 $20^3=7^3+14^3+17^3$，而对 $a=3$，$b=1$，有 $87^3=26^3+55^3+78^3$.

由另一种关系式可得到 $11^3+15^3+27^3=29^3$.

三个以上立方数之和为立方数的例子有：

$1^3+6^3+8^3=9^3=1^3+3^3+4^3+5^3+8^3$，

$11^3+12^3+13^3+14^3=20^3$，

$3^3+4^3+5^3+8^3+10^3=12^3=6^3+8^3+10^3$，

$1^3+5^3+6^3+7^3+8^3+10^3=13^3=5^3+7^3+9^3+10^3$，

$$2^3+3^3+5^3+7^3+8^3+9^3+10^3=14^3.$$

现已证明 $t<10000$ 时，$x^4+y^4+z^4=t^4$ 不可能. 但四个四次方数之和能等于一个四次方数，例如：$30^4+120^4+272^4+315^4=353^4$. 五个四次方数之和也有可能等于一个四次方数，例如 $4^4+6^4+8^4+9^4+14^4=15^4$. 对五个四次方数之和，有两个一般公式可利用：

$$(8m^2+40mn-24n^2)^4+(6m^2-44mn-18n^2)^4$$
$$+(14m^2-4mn-42n^2)^4+(9m^2+27n^2)^4$$
$$+(4m^2+12n^2)^4=(15m^2+45n^2)^4,$$

以及

$$(4m^2-12n^2)^4+(2m^2-12mn-6n^2)^4$$
$$+(4m^2+12n^2)^4+(2m^2+12mn-6n^2)^4$$
$$+(3m^2+9n^2)^4=(5m^2+15n^2)^4.$$

[290]

还有一个犹似一阵烟火的四次方等式：

$$1^4+3^4+4^4+5^4+9^4+10^4+11^4+12^4+14^4$$
$$+15^4+16^4+17^4+18^4+19^4+30^4=34^4.$$

方程 $x^4+y^4=u^4+v^4$ 具有众多解答，例如：

$$76^4+1203^4=653^4+1176^4,$$
$$59^4+158^4=133^4+134^4,$$
$$27^4+2379^4=577^4+729^4,$$
$$7^4+239^4=157^4+227^4,$$
$$193^4+292^4=256^4+257^4.$$

其中某些变量之间的通解公式为：$x=a+b$，$y=c-d$，$u=a-b$，$v=c+d$，此处

$$a=n(m^2+n^2)(-m^4+18m^2n^2-n^4),$$
$$b=2m(m^6+10m^4n^2+m^2n^4+4n^6),$$

$$c = 2n(4m^6 + m^4n^2 + 10m^2n^4 + n^6),$$
$$d = m(m^2 + n^2)(-m^4 + 18m^2n^2 - n^4).$$

也有可能继续推广到五次方与六次方的情况：

$$4^5 + 5^5 + 6^5 + 7^5 + 9^5 + 11^5 = 12^5$$

以及

$$1^6 + 2^6 + 4^6 + 5^6 + 6^6 + 7^6 + 9^6 + 12^6 + 13^6 + 15^6 + 16^6 + 18^6 + 20^6 + 21^6 + 22^6 + 23^6 = 28^6.$$

*　　　*　　　*

费马大定理不过是一大批不可能有解的方程之一，所不同的是，其他方程的不可能性都已完全证明. 例如 $x^4 - y^4 = z^2$ 是不可能有解的，$x^2 + y^2$ 与 $x^2 - y^2$ 不能同时为平方数. 毕氏三角形的面积 $2mn(m^2 - n^2)$ 不可能是一个平方数，也不是平方数的二倍，$x^2 + y^2 = ku^2$ 与 $x^2 - y^2 = kv^2$ 不能同时存在. 联立方程 $x^2 + ky^2 = u^2$ 与 $x^2 - ky^2 = v^2$ 对"同余数"k 的一些值可能有解，但具体求解通常都是十分困难的（见第 15 章）. 肯定不能求解的情况是 $x^4 + 4y^4 = z^2$ 与 $x^4 - 4y^4 = \pm z^2$.

然而这些结果对解决费马大定理问题都一点帮不了忙. 石城屹立，无法攻破，倔强的研究者们仍在勤奋地工作，时而在这里拿掉一块花岗岩，时而又在那里打开一个缺口. 某些出类拔萃的智力巨人丢番图，费马，高斯之类有本事穿城而过. 由此，人们衷心希望创造一个新的前沿阵地，以便对未知世界作进一步的探索. [291]

*　　　*　　　*

在我们走马看花，一带而过的数字世界里，从来没有破坏性的战争，也没有虚荣和物欲. 人们总是能够在那里安静休养，把吵吵闹闹的现实世界拒之门外. 这算不算逃避现实生活呢？也许

是的.不过,这总要比冒着风险,正面观看美杜莎[①]要好一些.高斯几乎是终生把自己关在哥庭根实验室的圣殿里,如果有更多的人像他那样真诚,谦虚,不摆架子,对一切事情看得很穿,那么这个世界也许就会好过得多.

正如E·T·贝尔在其著作《数学精英》里说的话:"这些令人鼓舞的观念,其中有的具有强烈同化作用,好像大热天喝冰水,足以使人神志清醒,又像是艺术,使人感到鼓舞."作者在本书正文行将结束之际,真诚地希望读者们也有同样的感受.

参考文献

Ball, W. W. R. *Mathematical Recreations and Essays*. New York: Macmillan Co., 1939.

Barlow, P. *Theory of Numbers*. London: J. Johnson & Co., 1811.

Bell, E. T. *The Last Problem*. New York: Simon and Schuster, 1961.

Cajori, F. *A History of Mathematics*. New York: Macmillan Co., 1919.

Carmichael, R. D. *Theory of Numbers and Diophantine Analysis*. New York: Dover Publications, Inc., 1959.

Cashmore, M. *Fermat's Last Theorem*. London: G. Bell & Sons, 1916.

Dantzig, T. *Number: The Language of Science*. New York: Macmillan Co., 1930.

Dickson, L. E. *History of the Theory of Numbers*. 3 vols. New

① 美杜莎是希腊神话中的蛇发女怪,被其目光扫到者即化为石头.——译者注.

York:Chelsea Publishing Co. ,1950.

——. *Introduction to the Theory of Numbers*. New York:Dover Publications,Inc. ,1957.

——. "Fermat's Last Theorem and the Origin and Nature of the Theory of Algebraic Numbers,"*Annals of Mathematics*, Series 2,**18**(1917),161.

Hardy,G. H. "An Introduction to the Theory of Numbers," *Bulletin of the American Mathematical Society*,**35**(1929), 778.

Heath,T. L. *Diophantus of Alexandria*. London:Cambridge University Press,1910. [292]

Lehmer,D. H. ,and Lehmer,E. "A Note on Fermat's Last Theorem,"*Bulletin of the American Mathematical Society*, **38** (1932),723.

——. "On the First Case of Fermat's Last Theorem,"*Bulletin of the American Mathematical Society*,**47**(1941),139.

Mordell,L. J. *Three Lectures on Fermat's Last Theorem*. London:Cambridge University Press,1921.

Pierce,G. W. *Greater Fermat Theorem Proved*. Boston:G. W. Pierce,1914.

Rosser,B. "On the First Case of Fermat's Last Theorem,"*Bulletin of the American Mathematical Society*,**45**(1939),636.

Smith,H. J. S. "Report on the Theory of Numbers,"*British Association for the Advancement of Science*,**30**(1860),120.

Uspensky,J. V. ,and Heaslet,M. A. *Elementary Number Theory*. New York:McGraw-Hill Book Co. ,1939.

Vandiver,H. S. "Note on Some Results Concerning Fermat's Last Theorem,"*Bulletin of the American Mathematical Society*,**28**(1922),258.

——. "Fermat's Last Theorem," *American Mathematical Monthly*, **53**(1946), 555.

Vinogradov, I. M. *Elements of Number Theory*. New York: Dover Publications, Inc., 1954.

Walsh, C. M. *An Attempted Proof of Fermat's Last Theorem by a New Method*. New York: G. E. Steckert & Co., 1932.

[293]

第25章 马上比武[①]

1. 有人收到一张支票，但在兑付现金时，银行出纳员把元数与分数搞颠倒了．其人当时没有发现错误，在他用去68美分后才惊讶地察觉到：剩下来的钱数竟是支票上所开金额的二倍．试问，所开支票的最少钱数应是多少？

2. 森地·麦克阿列斯特答应送给他妻子一件漂亮礼物，如果她能够节省下足够多的银币，使之能排成正方形（例如4枚或9枚），1个正三角形（3枚或6枚），或者2个三角形，3个三角形．试问她至少应储蓄多少枚钱币？平凡解$1美元不能算数．

下一年，他又重新作了承诺，但坚持要求她这次省下的钱数应与上次不同．就这样一直维持了六年．试问：她每年省下多少钱？

3. 三块正方形板，其边长的英寸数都是整数．第二块板的面积比第一块要多出5平方英尺，但却比第三块小5平方英尺．求三块板的大小．

4. 两所教堂的钟在同时打响．第一所教堂的钟每经4/3秒响一声，而第二所教堂打钟的间隔为7/4秒．试问：在15分钟内可听到多少下钟声？但要注意，间隔在$\frac{1}{2}$秒以下或更短的两记钟声无法分辨，是要被认作同一声的．

---

① 最后一章中有这些问题的解法．——原注．

5. 求满足关系式 $x^2+y^2=z^2+1$ 的整数解.

6. 有一条由 12・12=144 个补片缝缀起来的被子,试将它分为 11 块,每块的形状都是正方形,且都不少于 4 个补片.

7. 求一最小平方数,使之为三个以上连续数的立方之和,[294] 但其中不能有 1 的立方.

8. 试找出一个能使毕氏三角形的斜边为平方数的公式.

9. 设金刚石的价格与其重量的平方成正比,红宝石的价格则与四次方成正比.一克拉的金刚石与一克拉的红宝石,其价格分别是 1000 与 2000 美元.有一位珠宝商想用一对耳环(由同类宝石镶嵌而成)同别人的两块重量不同的宝石进行交换.如果宝石重量的克拉数统统都是整数,试求出交换的各种可能情况,宝石重量的最小数及其价值.

10. 某牲畜贩子赶着五大群动物,每群都有着同等头数的猪、牛、羊.他把它们悉数卖给了八个商贩.每个商贩都买了为数一样的牲畜,代价是:每头牛 17 美元,每头猪 4 美元,每只羊 2 美元.牲畜贩子一共收进 301 美元.试问:牲畜贩子最多可能有多少动物,每种各是多少?

11. 求周长为平方数的本原毕氏三角形.

12. 两支人数不等的部队,各自拥有的将士数都是平方数.将军自己也包含在一支队伍之内.将开赴前方作战时,他们经过重组,把全体人员列成一个方阵.但他们的领袖则留在 10 英里外的山顶上以护卫后军.试问:若总数恰在十万以下,这两支部队的原来人数各是多少?

13. 某人有 6 只桶,其容量分别为 15,16,18,19,20 与 31 加仑.5 只桶里装的是酒,1 只桶里装的是啤酒.他把一部分酒售与一位买主,另一买主则买了前者所买的二倍,这样一来就只剩下装满啤酒的一桶了.试问,在 6 桶中,装啤酒的是哪一桶?

14. 在 10 个数码中挑出 9 个,能为 11 整除的最大数与最小数各是多少?

15. 在公元 x^2 年，某人年龄是 x 岁. 试问：1960 年，他是几岁？

[295]

16. 试将下面开方算式中迷失的数字加以复原：

```
        -   -   -   -
    √ - - - - - - - - -
        -
      ----
        - - -
          - -
        -----
          - - - -
          - - - -
          -------
            - - - - -
            - - - 3 -
            ---------
```

17. 求一最大除数，用它去除四个数 701；1059；1417；2312 时能得出相同的余数.

18. 求能使 $x(x+180)$ 为一平方数的一切正整数 x.

19. 某人到银行里去兑现一张 200 美元的支票，要求行员给他若干张 1 美元钞票，2 美元钞票的张数为前一种钞票张数的十倍，剩下来的钱可给他 5 美元钞票. 试问：银行工作人员是怎样满足其要求的？

20. 琼尼对他朋友汤米说："我有一些弹子，其个数为平方数. 把你的弹子给我一些，则我有的弹子个数将是另一个平方数."汤米答道："我知道你需要多少弹子. 但若你给我这些数目的弹子，你剩下来的弹子数仍将是一个平方数."试问，琼尼至少应有多少粒弹子？

21. (a)三块正方形板，其面积成等差数列，公差是 7 平方英尺，边长为有理数. 试求各块板的大小.

(b)公差为 13 平方英尺时，试解此题.

(c)公差为 23 平方英尺时,试解此题.

22. 三只藏宝箱里各装着为数不等的金币,中间箱子与上面箱子里的币数之差正好等于下面箱子与中间箱子里的币数之差. 任何两只箱子里的金币数之和是个平方数.

(a)在币数最少的那只箱子里,满足题设条件的金币的最小数是多少?

[296] (b)最小的金币总数是多少?

23. 在某条街上,门牌号码从 1 号开始. 有人注意到,把直到他家为止的门牌号码统统加起来(他家本身的门牌号码不在其内),其和正好等于超过他家门牌号的各家门牌之和. 试求他家的门牌号码,若它大于 100 而小于 1000 的话. 倘若门牌号码是从 1 开始的连续编号,而不是通常的隔号编法,试解同样的问题.

24. 比尔与弗来德把他们的 30 件脏衬衫送到洗衣房. 弗来德打电话给洗衣房,对洗衣工说,他的那一包里只有尼龙衬衫总数的一半,棉衬衫总数的三分之一,所以洗衣费只要 3.24 美元就够了. 4 件尼龙衬衫的洗衣费相当于 5 件棉衬衫. 不具备东方人精明头脑的洗衣工霍普·阿龙想知道比尔那一包衣服应收多少洗衣费?

25. 某人去世时的年龄正好等于他出生那年公元年份数的 1/29. 试问,在 1940 年时,此人有几岁?

26. 威格斯太太的正方形菜地今年比去年多收了 211 棵卷心菜. 试问她究竟收了多少?

27. 数 $90ABC17$;$79ABC$;$491ABC4$(其中字母代表模糊不清的数字)具有一个公因数. 试把这些数统统求出来.

28. 一块直角三角形土地,一边之长为 47 个标准轨长. 试问:要用多少根标准轨,才能把它全部围起来?

29. 某人有 6 桶容器,装着酒或啤酒. 其容量分别为 8,13,15,17,19,31 加仑. 一个买主各用 28 美元分别买了这两种饮

料，酒价是啤酒价的二倍.这时，店主只剩下了一桶饮料.试问，它值多少美元？

30. 若干年以前，一位热情的乡下情郎告诉他的女朋友，"一周前的星期二是'明天'时，你曾说过，'从今日算起，第28天是'昨天'时，我们就可以结婚了，因为那一天正好是下个月的同一日期.'现在，亲爱的，我们已经等待了正好二星期，而它已是这个月的第二天，让我们来算一算我俩的大喜日子吧."

31. 两人有同样多的钱，参加赛马赌博.他们把赌注押在最蹩脚的马身上，因为赔率极高，区区一元钱可赢得很多的钱.汤姆把赌注押在一匹绰号"硬饼干"的马匹上，认为它可得第一名，比尔也押在它上面，认为它可得第二.他们下的赌注不一样，赔率也不一样，但两个赌注合在一起，相当于共有资本的一半.最后两人都赢了.但清点以后，发现汤姆的钱数是比尔的二倍.试问，他们赢了多少钱？ [297]

32. 现做现卖的小贩在沿街叫卖：

"好吃的十字架面包[①]，又热又香又甜，

一个铜板买一只，一个铜板买二只.

姑娘们不爱吃，那就买来哄小子！

一个铜板买二只，一个铜板买三只.

我的儿女一样多，

给他们七个铜板买来吃."

如果各个孩子不分男女都一视同仁，而且买小圆面包的办法只有一种.试问：一共有几个孩子？

33. 一个三角形湖泊的周围被三家正方形庄园所环绕，如果庄园的面积分别为74，116与370英亩.试求湖泊的面积.

34. 求满足下列方程的最小整数解：

(a) $x^2-1620y^2=1$，

① 在耶稣受难日吃的，上面做有十字架图案的圆形小面包.——译者注.

(b)$x^2-1666y^2=1$.

35. 汤姆,威利,玛格丽,安妮用 40 美分买了 20 块糖果. 已知一块樱桃糖值 8 美分,果汁糖 1 分可买两块,杏仁巧克力糖 1 分一块. 如果每个孩子分到的糖果完全一模一样,试问钱数应怎样支配?

36. 有个家伙参加轮盘赌,他先用 1 个法郎赌 7 次,不问是输是赢,接着用每次 7 法郎赌 7 次,然后又是每次 49 法郎赌 7 次,……总而言之,他的赌注都按照 7 的乘幂逐步加码……如果他最后赢了 777777 法郎,试问他赢过几次?

37. 某男孩有一批椰子,原来堆成两座三角形底的圆锥形宝塔,现在要改为一座三角形底的圆锥形塔. 试问,他至少要有多少颗椰子?

38. 某人有 100 多枚硬币,其个数正好是一平方数,他把硬币分成相等的 19 堆,每堆的个数都是平方数,剩下 81 枚硬币. [298] 试问他至少拥有多少枚硬币,并给出一个通解公式.

39. 有个守财奴窖藏着一批金币,其面值分别是 5 元,10 元与 20 元三种. 老头子把这些金币放在 5 只口袋里,每袋内容完全相同. 他把玩着这些宝货,并将它们分成完全一样的 4 堆. 然后,在确信一枚钱币都未丢失的情况下,他拿起了两堆并将它们分成完全一样的 3 堆. 试问,在这个可怜虫活活饿死之前他到底藏着多少钱财?

40. 旅行家与导游没命地冲上大金字塔狼狈逃命,后面紧追着一头狮子. 旅行家一次跨 5 级,导游一次可跨 6 级,而狮子则一次跨 7 级. 在某一瞬间,旅行家与塔尖只差 1 级,导游还差 9 级,而狮子则相距 19 级. 试问大金字塔共有几级?

41. 某人跑进店里,花掉了他口袋里的一半钱,当他出店时他发现剩下来的分数等于他进店时的元数,而剩下来的元数只有进店时分数的一半. 试问,他进店时,口袋里有多少钱?

42. 一位中国贵妇人想买一头价值 11 元的小狗. 已知 11

枚圆孔铜钱值 15 元;11 枚方孔的铜钱值 16 元,而 11 枚三角形孔的铜钱值 17 元.试问:为了买这只狗,各种铜钱要用多少?

43. 把 1961 这个年数用八进位制来表示.

44. 一只鸡蛋重 2 英两,可支撑 8 磅重量.试问,可堆成多少高的底为正方形的一座锥形塔而不出风险?如底为三角形,可堆成多少高?

45. 求一毕氏三角形,其三边成算术级数.

46. 一个 13×13 的正方形至少应分成多少个小正方形,并可将它们重组为两个正方形?

47. 若连续三数的中间一数为立方数,试证此三数的乘积必能被 504 整除.

48. 求不超过 100 且具有同样的 $\phi(N)$ 的一切自然数 N(至少要有两个).$\phi(N)$ 是小于 N 且与 N 互质的整数的个数.

49. 若 N 仅有一个素数除数,试解问题 48.换言之,试求素数 p,q,指数 a,b,使 $\phi(p^a)=\phi(q^b)$ 成立. [299]

50. 一位酒商有 5 只立方体大桶,每只桶的边长为 9 英尺.他还有 15 只较小的容器,其形状也是立方体.有两只容器的大小尺寸一样.他把 3 只小容器中的酒全部倒入大桶中使其灌满,试求各容器的大小.

51. 求一个不到 40 位的七进制数,使数码 3 从最右边移到最左边时,所得之新数(仍是一个七进制数)是原数的 $\frac{4}{5}$.

52. 一个行为乖张的大富豪要把一百万元送人,赠款是 1 元或 7 的乘幂,例如 7,49,343,2401 元等等.他最不喜欢有 6 人以上拿到一样的赠款,但却不计较有多少人要领取赠款.试问,这一百万元应如何具体分配?

53. 荒岛上有 n 个乘船遇难者,一只猴子.他们采集了一堆椰子,准备在下一天瓜分.半夜里一个人悄悄起来,把椰子分作相同的 n 份,发现多出一只椰子,此人把它丢给猴子吃了.然后

他藏起了一堆.其他人也重复了这种行径.最后一人所留下的椰子正好可以分成 n 份.试问:原有多少椰子?若有 r 只猴子,此题应如何求解?

54. 求一个最小的,只含数码 3 与 7 的整数,要求这个数以及它的各位数码之和都能被 3 与 7 整除.

55. 求一个只含 3,5,7 的最小整数,要求此数以及其各数码之和都能被 3,5,7 整除.

56. 求一个最小的整数,其中 10 个数码都各出现一次,要求此数能被 1,2,…,7,8,9 整除.

57. 求出两直角边为连续数的前 100 个毕氏三角形.

58. 一位土耳其苏丹打算派出一支部队去打仗,其人数可用 12 种不同办法形成两个方阵.试问,至少要有多少人才能办到,具体应如何安排?

59. 约翰·史密斯船长于 1803 年在格罗塞斯特郡病故,他[300]生前做过奴隶交易,死后留下一笔相当可观的遗产给他的九个继承人,五男四女.这些人是:已婚儿子,他的老婆、孩子;已婚的女儿,她的丈夫、孩子;已婚的继子和他的妻、儿.遗嘱规定每个丈夫所分到的钱要多于其妻子所得,而妻子的钱又多于小孩的钱,对此三家来说,差数都一样.所分之钱统统都是一元钞票,每个继承人都拿到一包密封信件,而每只信封里的一元钞票张数等于他或她所得小包中的信件份数.继承人的名字叫比尔、玛丽、汤姆、爱莉莎、亨克、苏珊、奈特、莎拉、杰克.玛丽与莎拉拿到的钱同汤姆与比尔拿到的钱一样多,而奈特、比尔、玛丽在一起所拿到的钱要比亨克多出 299 美元.贫穷的琼斯家要比布朗家多得三分之一.问各位继承人姓甚名谁?

60. 某数 N 的末位数 D 移至首位后,形成的新数将是原数的 K 倍.试就 $K=2,3,\cdots,D=2,3,4,\cdots,9$ 等情况,求出数 N 及其位数.

61. 在兑现一张 4 位数支票时,银行出纳员错误地支付了

一笔由原数的逆序数所表示的现金.从而造成亏损,而亏损金额是一个平方数.(a)此种平方数可能有多少个?(b)它们究竟是哪些数目?(c)原来所开出的支票可能有多少种不同写法?

62. 如果上题的亏损金额是一个立方数,试解相应的问题.

63. 数 $N=AAABBBCCC$,加上1以后,它变成了一个平方数,试求 N.(A,B,C 是不同数字.)

64. "漂亮姑娘名丽琳,
从1加到十亿整.
各位数字都要加,
总和多少算分明.
此事实在太烦心.
你能助以一臂力,
她愿酬谢百万金."

65. 若 x 为一正整数,试证明 $3^{2x+1}+2^{x+2}$ 恒能被7整除.

66. $(EVE)/(DID)=0.TALKTALKTALK\cdots$ 表示一个已化成循环小数的普通分数.试说出各字母所代表的数字. [301]

67. 设 ABC 为一毕氏三角形,BF 是直角 B 的分角线.垂线 AE 与 BF 相交于 E.G 是斜边的中点,GE 与 AB 相交于 D.线段 EG 之长等于49.求三角形 ABC 的各条边.

68. 一个三位数除以其各位数字之和时得出商数26.求满足此条件的最小数.

69. 求一最小整数,它能用7种不同方法表示为两个整数的平方和.

70. 求出以 $aabbccddee$ 代表的两数,其中之一为完全平方数,另一个是完全平方数加上7.每种情况均有两个解答.(由不同字母代表的数码不一定要求不相同,然而同样的字母必须代表同样数码.)

71. 两个人出售一群母牛.母牛共计 x 头,每头售价 x 元.他们用售牛收入买进若干头绵羊,每只羊进价10元,还有一只

小羔羊，进价不足10元.每人都分到了同样头数的动物，但为了使分配公正无欺，分到小羔羊的人另外收进了一些补偿金.试问，他将从另一人手上拿进多少钱？

72. 人数略少于500万的一支大军排成一个庞大的方阵，另外又得到了十个方队的人员增援.这十个方队，每队都拥有同等数量的将士.现在整个部队的总人数超过了一千万人，但少于原先人数的3倍.现在他们可以排成400个同样的方队，或者全体人员排成一个方阵.试问：在400个方队中，每队各有多少名将士？

73. 在一张陈年旧发票上记载着：买进72只火鸡，总价 *67.9* 美元；首位与末位数字已经分辨不清了.试求出这些数目字.

74. 数$(abbbb)^2-1$有着十位数码，不重不漏.求此数.

75. 求一最小与最大的平方数，使所有的十个数码全都出现，而且每个数码都只出现过一次.

76. 利用不重复的十个数码，试求出一个10位数，此数在加上一百万以后，可得出一个平方数.后者的平方根必须是一个回文数，即顺读和倒读都相同的数.

77. 在删去数码0的条件下解第76题，此时所涉及的将是
[302] 一个九位数，其他条件都同上题一样.

78. 不考虑问题76与77中所提的回文数要求，试求以上两题的解，使两个5位数的平方根把10个数码全都用上.

79. 人口普查员询问在走廊里遇到的男人：这屋子里住着哪些人以及他们的年龄.此人答道："我的年龄是我老婆、儿子、女儿年龄之和，我们的年龄全都是平方数.我父亲的年龄是我的年龄再加上我老婆与女儿的年龄，尽管他早已过了壮年，可是他的年龄却是一个素数."人口普查员不慌不忙地作了记录.对这户人家中妻子的年龄，他应当作些什么特殊注解呢？

80. 试证 $1+[1+(10^{10}-1)^{99989}](10^{999890}-1)\equiv 0$,

mod 99991.

81. 一位农夫有块土地，其形状很像正五边形. 五条边中的每一条也都是毕氏三角形中的一边. 所有五个三角形都不相似，而其顶点都在农夫庄园的外面. 试问，五块三角形土地至少应有多大面积？而农夫的土地，面积又应是多少？

82. 出售电子零件的年度毛收入是 3893.93 美元，上一年的生意要好得多，毛收入是 8311.19 美元. 设零件售价保持不变，试问：上一年卖出了多少零件？

83. 一位年老的炼金术士有两个球形烧瓶，其中一只周长 12 英寸，另一只周长 24 英寸. 他想把其中的液体倒入另外两只大小不一样的烧瓶中去，而后者与原先的两只烧瓶大小也不相同. 试问，若用有理数表示，两只新烧瓶的周长各是多少？

84. 汽车代理人发现，他们出售某种汽车的年度总收入是 1,111,111.00 美元，但究竟卖出了多少辆汽车的原始记录却找不到了. 你能不能帮他一点忙？

85. 一个商人有两只大小不一样的立方体盒子，其容积之和为 6 立方英尺. 求两只盒子的大小.（用有理数表示.）

86. 一农夫拥有一块正方形土地，每边长为$\frac{5}{4}$英里. 他为四个儿子在四只角上搭起了篱笆，围成了直角三角形土地. 这些三角形有着相同面积，但其形状都不一样. 三角形各边之长，以英尺表示时都是整数. 截出四角后，留下来的土地，其形状是一个不规则的八边形，但仍拥有原来正方形土地面积的 96%以上. [303] 试问：其面积到底有多少平方英尺？

87. 求具有同样周长的四个最小本原毕氏三角形.

88. 求一个九位平方数 $N^2=abcdefabc$，它的平方根是四个不同素数的乘积，此处，$a\neq 0$，而$(def)=2(abc)$.

89. 求最小的三个连续整数（0 要排除在外），其中每个数都是两平方数之和.

90. 某个 8 位数 273 * 49 * 5 中有两个数码被涂掉了. 已知该数能被 9 与 11 整除. 求迷失的数码.

91. 在一个动物饲养场里,马与小鸡的头数与翅膀数之和等于足数. 问:场里有多少匹马,多少只小鸡?

92. 某学生不小心擦掉了一个除法的竖式算草,他只能回忆得起,由上往下的紧挨着的被减数是 690;2415 与 2070,而最后的余数是 1. 根据这些信息他复原了原来的草式. 你也能做到吗?

93. 一个七进制的三位数在转换为九进制时,三个数码正好颠倒过来(还是这三个数码,但顺序从自左到右变成自右到左). 试求此数.

94. 对一切整数 x 值,试证明 $\frac{1}{5}x^5+\frac{1}{3}x^3+\frac{7}{15}x$ 恒为整数.

95. "给我求出一个数来,"国王对他的宫廷弄臣说,"它的一半应是一个平方数.""这太容易了,"小丑说."但是,它的三分之一应是一个立方数."国王继续说下去,小丑看来脸色沉重了."最后,此数的五分之一应该是一个五次方数."小丑一听,简直要昏倒了."明天早上你一定要找出这个数目,"国王最后斩钉截铁地说,"否则你就得把我寡居的老岳母领去,同她结婚."弄臣被国王彻底击溃了,总算下一天早上他求出了正确答案,从而摆脱了比死还要糟糕的坏运气.

96. 求一立方数,使它在减去一平方数后,其差等于 2,000,000.

97. 证明 $61!+1\equiv 0$,与 $63!+1\equiv 0 \mod 71$.

98. 当且仅当 $(n+1)$ 不是一个素数时,前 n 个连续自然数的乘积能被其和整除,试证明之.

[304] 99. 在 10000! 尾部有多少个紧接着的 0?①

① 原文提法不严密,现改正如上. ——译者注.

100. 一个等腰三角形的两边都等于某一本原毕氏三角形的斜边. 试证明:存在着另一直角三角形,其直角边之长为整数,而其斜边等于该等腰直角三角形的斜边. [305]

第26章　女王的讲解：问题的解答与提示

第1章的问题

第1页[1]

1. $16000001=109\cdot229\cdot641$.

2. 见111页的图4.

3. 由于 $5929=7^2\cdot11^2$；小于此数并与之互质的整数的个数是 $\phi(5929)=7\cdot6\cdot11\cdot10=4620$.

4. 见323页，第25章问题54的解答.

5. 若 $x=p^2-q^2-2pq$，$y=p^2+q^2$，$z=p^2-q^2+2pq$（p，q 为整数），则 x^2，y^2，z^2 成算术级数. 如令 $p=2$，$q=1$，这些数目是 -1；5；7 而其平方数为 1；25；49. 当 $p=3$，$q=1$ 时，这些数目是 2；10；14 而其平方数为 4；100；196. 四个平方数是不能成为算术级数的.

6. 见第2章的问题解答.

7. 见第7章.

8. 可参看一本数论教科书，例如乌思宾斯基与希斯莱特的《初等数论》，美国麦克格劳图书公司，1939年出版.

9. 见第3章.

---

[1] 指原书页码，下同；今后不再注明. ——译者注.

第 2 章的问题

第 8 页

1. 求具有 100 个除数的最小数. 把 100 分成 2,3,4 个除数的乘积:50・2,25・4,20・5,10・10;25・2・2,10・5・2,5・5・4;5・5・2・2. 由此得出 100 个除数的相应形状为:$p^{49}q$、$p^{24}q^3$、$p^{19}q^4$,p^9q^9;$p^{24}qr$,p^9q^4r,$p^4q^4r^3$;p^4q^4rs. 由最后一个形式可得出最小解 $2^4\cdot3^4\cdot5\cdot7=45360$.

2. 求具有 96 个除数的最小数. 先把 96 分成 2,3,4,5,6 个因子的乘积. 我们只需检查 5 个与 6 个因子的两种情况,因在其他情况之下,相应的指数必然十分庞大,肯定得不出最小解. 这 [306] 就需要考虑 6・2・2・2・2;4・3・2・2・2;以及 3・2・2・2・2・2 等情况,与此对应的数其形式为 p^5qrst,p^3q^2rst,p^2qrstu,它们将引出解答

$$2^5\cdot3\cdot5\cdot7\cdot11,\ 2^3\cdot3^2\cdot5\cdot7\cdot11,$$
$$2^2\cdot3\cdot5\cdot7\cdot11\cdot13,$$

其中以第二数 $2^3\cdot3^2\cdot5\cdot7\cdot11=27720$ 为最小.

第 5 章的问题

第 35 页

求魔数 715;364;924(或 5,4,−1),设 X 为未知数,p,q,r 为待定之魔数. 令 a,b,c 分别为 X 对模 7,11,13 之剩余,则有 $pa+qb+rc-K\cdot1001=X$. 令 $p=11\cdot13u$;$q=7\cdot13v$;$r=7\cdot11w$,则 $143ua+91vb+77wc-X=1001K$. 于是有

$$3ua-a\equiv0 \mod 7,$$
$$3vb-b\equiv0 \mod 11,$$
$$12wc-c\equiv0 \mod 13.$$

由于 a,b,c 分别与 7,11,13 互质,我们可在同余式中约去公因

子，从而得出：

$$3u \equiv 1 \mod 7,$$
$$3v \equiv 1 \mod 11,$$
$$12w \equiv 1 \mod 13.$$

于是 $u\equiv5$，$v\equiv4$，$v\equiv12$，分别对应于模 7，11，13. 因此 $p=143u=715$；$q=91v=364$；$r=77w=924$.

如果不用 p、q、r，只要记住 $u=5$，$v=4$，$w=12$（或 -1），也可像第 5 章正文中所讲的那样，得出这些魔数.

第 38 页

1. $x=37a-1$；$y=83-71a$，这里，a 是任一正、负整数或零.

2. $x=11+107a$；$y=873-599a$，这里，a 是任一正、负整数或零.

3. $1001x+770y=1000000+b$. 除以 77，可得出 $13x+10y=12987+(b+1)/77$，可见 $b=76$ 是可使分式给出整数值的最小值. 于是 $10y\equiv1 \mod 13$，$y\equiv4 \mod 13$，即 $y=13z+4$. 故有 $13x+130z+40=12987+1$，除以 13 后，得出 $x+10z+3=999$，即 $x=996-10z$. 可见，在 z 的值取 0 到 99 时，能得出 100 个解 [307] 答.

第 6 章的问题

第 47 页

我们必须去解

$$(2^{p-1}-1)/p=a^2,$$

也就是

$$2^{p-1}-1=pa^2=(2^{(p-1)/2}+1)(2^{(p-1)/2}-1).$$

如果括号内的数量有一个公因子，则其差 2 便是一个. 但是这些

数量都是奇数,因此,除 1 之外,它们不可能具有公因子 2. 由此可知它们必为互质数,由于其乘积为 pa^2,所以其中之一必为平方数,否则它们不可能互质. 从而可以肯定,或者是 $2^{(p-1)/2}+1=x^2$,或者是 $2^{(p-1)/2}-1=x^2$,两者必居其一. 如为前一情况,因 x 是奇数 $=2y+1$,故有

$$2^{(p-1)/2}+1=4y^2+4y+1,$$

即
$$2^{(p-1)/2}=4(y^2+y)=4y(y+1).$$

由于 y 与 $y+1$ 中必有一个奇数,故其乘积不可能是 2 的幂,除非 $y=1$,其时相应的 p 等于 7. 在后一情况,$2^{(p-1)/2}-1=4y^2+4y+1$,即 $2^{(p-1)/2}=2(2y^2+2y+1)$,括弧中的数量是个奇数,而当奇数的二倍是 2 的乘幂时,这个奇数只能是 1,由此可知 $y=0$,相应的 p 值为 3. 因此当 $p=3$ 与 7 时,费马商才是平方数,它们分别是 1 与 9.

第 8 章的问题

第 57 页

哪个和数更大些?

1 2 3 4 5 6 7 8 9	1
1 2 3 4 5 6 7 8	2 1
1 2 3 4 5 6 7	3 2 1
1 2 3 4 5 6	4 3 2 1
1 2 3 4 5	5 4 3 2 1
1 2 3 4	6 5 4 3 2 1
1 2 3	7 6 5 4 3 2 1
1 2	8 7 6 5 4 3 2 1
1	9 8 7 6 5 4 3 2 1

两个和数一样大.

第 60 页

数 $111222333444555666777889=(1/81)(1/111)\cdot 10^{27}$

$=(1/9)\cdot(1/111)\cdot(111111111111111111111111111)$

[308] $=(1/9)\cdot(1001001001001001001001001)$.

第 62 页

为什么 15873 与 7 的倍数相乘时能得出一串重复数码呢？数 $15873=3\cdot11\cdot13\cdot37$，因而 $7m\cdot15873=m(7\cdot11\cdot13)(3\cdot37)=m\cdot1001\cdot111=m\cdot111111$.

为什么 $90991\cdot123321$ 能给出 111111111111？这是因为 $90991=9901\cdot7\cdot13$，而 $123321=1111\cdot111=101\cdot11\cdot3\cdot37$. 于是

$$\begin{aligned}90991\cdot123321 &= (9901\cdot101)(7\cdot11\cdot13)(3\cdot37)\\ &= 1000001\cdot1001\cdot111\\ &= 1000001\cdot111111\\ &= 111111111111.\end{aligned}$$

第 65 页

除 2 与 5 之外，为何一切素数都能整除无限多个由同一数码重复而形成的整数？由费马定理可知，如果 p 是 2 与 5 以外的其他素数，则同余式 $10^e\equiv1 \mod p$ 恒有一解(见第 10 章). 因而，$10^e-1=99\cdots9$(e 个 9 不断重复而形成的整数)必能为 p 整除.(能为 p 整除的、个数最少的一串 9，其个数是模 p 时 10 所属的指数，而 e 的任何整倍数所形成的一串 9 都能被 p 整除.)

由于任一素数都与其他素数互质，我们可将一串 9 所形成的数除以 9，从而得出一串 1，而这不会影响可除性. 最后，又可把这一串 1 乘以任何其他 7 个数码之一而不影响可除性. 换言之，由一串同样数码所形成的整数恒能被一素数整除，只要有足够多的重复数码就行(最多不超过 $p-1$ 个).

第 12 章的问题

第 89 页

把 10 写成公式 B 的形式可以有两种办法，它们是：

$$11^0(11-1),\quad 2^0(2-1)11^0(11-1).$$

对数2而言，则有$2^1(2-1)$，$3^0(3-1)$，$2^0(2-1)\cdot 3^0(3-1)$.

第91页

Ⅰ. 设$b=\phi(N)$. 将b用一切可能办法记为公式B的形状.

(1) 令$b=2^aQ$，此处Q是奇数. 在f为首的一列里，列举出b的偶除数f_i，但含2^a的那些除数不在其内. 注意，1与b本身也应列入.（为了便于核查，防止遗漏，应将每个除数都写成素数的乘幂之连乘积.）

(2) 在以A为首的第二列中，要记下各个(f_i+1)的值，如果它们是素数的话，否则，记为“—”，以表示空缺.

(3) 将每个f_i用其最大素数B的最高次幂B^c去除，若商为$B-1$，则在B的一列中记下B^{c+1}；若商不等于$B-1$，则记下空缺号“—”.

[309]

(4) 在A列或B列中一处都未出现过的f_i应予排除.

(5) 从f列中选取因子，将b用一切可能办法表为1，2，3，…，直至$(a+1)$个因子的乘积，所采取的只能是试探办法. 1必须视为一个不同因子. 一个因子f_i只能在乘积中再重复一次，在A与B两列里不能同时出现两个空缺记号.

如在A列与B列中对应的素数完全一样，则应排除此种因子组合. 例如在表99中，不能同时都要$2\cdot 5$与$2\cdot 5\cdot 11$这样的组合，因与这种因子组合对应的素数都是11或其乘幂.

(6) 为了把b表为公式B的形状，把(5)中用到的每个f_i写下来. 若A列中有一空缺，则记下$A_i^0(A_i-1)$；B列中有一空缺，则记下$B_i^c(B_i-1)$. 这些值应表达成连乘积. 若A，B两列中都出现空缺，则f_i可提供两解.

第91页

Ⅰ. 把Ⅰ的结果记在$\phi(N)$的这一列. 在N这列中，则把N_i写成$A_i^0(A_i-1)$与$B_i^c(B_i-1)$的连乘积. 实例：对

$$b=\phi(N)=2^3\cdot 3\cdot 5^2\cdot 11.$$

具体解法详见表 99 与 100.

f	A	B	f	A	B
1	2	—	$2\cdot 3\cdot 5^2\cdot 11$ *	—	—
2	3	2^2	$2^2\cdot 3$	13	—
2^2	5	2^3	$2^2\cdot 5$	—	5^2
$2\cdot 3$	7	3^2	$2^2\cdot 11$ *	—	—
$2\cdot 5$	11	—	$2^2\cdot 5^2$	101	5^3
$2\cdot 11$	23	—	$2^2\cdot 3\cdot 5$	61	—
$2\cdot 5^2$ *①	—	—	$2^2\cdot 3\cdot 11$ *	—	—
$2\cdot 3\cdot 5$	31	—	$2^2\cdot 5\cdot 11$ *	—	—
$2\cdot 3\cdot 11$	67	—	$2^2\cdot 3\cdot 5^2$ *	—	—
$2\cdot 5\cdot 11$	—	11^2	$2^2\cdot 5^2\cdot 11$ *	—	—
$2\cdot 3\cdot 5^2$	151	—	$2^2\cdot 3\cdot 5\cdot 11$	661	—
$2\cdot 5^2\cdot 11$ *	—	—	$2^2\cdot 3\cdot 5^2\cdot 11$	3301	—
$2\cdot 3\cdot 5\cdot 11$	331	—	$2^3\cdot 3\cdot 5^2\cdot 11$ *	—	—

[310] **表 99 给出 $\phi(N)=2^3\cdot 3\cdot 5^2\cdot 11$ 时、求解 N 的准备工作**

$\phi(N)=b$ 作为 f_i 的乘积	取公式 B 形式的 $\phi(N)=b$（Ⅰ的解答）	N（Ⅰ的解答）
$(2)(2^2\cdot 3\cdot 5^2\cdot 11)$	$(a)\ 3^0(3-1)\cdot 3301^0\cdot(3301-1)$	$3\cdot 3301$
	$(b)\ 2\cdot(2-1)\cdot 3301^0\cdot(3301-1)$	$2^2\cdot 3301$
$(2^2\cdot 5)(2\cdot 3\cdot 5\cdot 11)$	$5\cdot(5-1)\cdot 331^0\cdot(331-1)$	$5^2\cdot 331$
$(2\cdot 5)(2^2\cdot 3\cdot 5\cdot 11)$	$11^0\cdot(11-1)\cdot 661^0\cdot(661-1)$	$11\cdot 661$
$(2\cdot 3\cdot 11)(2^2\cdot 5^2)$	$(a)\ 67^0\cdot(67-1)\cdot 5^2(5-1)$	$67\cdot 5^3$
	$(b)\ 67^0\cdot(67-1)\cdot 101^0(101-1)$	$67\cdot 101$
$(2\cdot 5\cdot 11)(2^2\cdot 3\cdot 5)$	$11\cdot(11-1)\cdot 61^0(61-1)$	$11^2\cdot 61$
$(1)(2)(2^2\cdot 3\cdot 5^2\cdot 11)$	$2^0(2-1)\cdot 3^0(3-1)\cdot 3301^0(3301-1)$	$2\cdot 3\cdot 3301$
$(1)(2^2\cdot 5)(2\cdot 3\cdot 5\cdot 11)$	$2^0(2-1)\cdot 5(5-1)\cdot 331^0(331-1)$	$2\cdot 5^2\cdot 331$
$(1)(2\cdot 5)(2^2\cdot 3\cdot 5\cdot 11)$	$2^0(2-1)\cdot 11^0(11-1)\cdot 661^0(661-1)$	$2\cdot 11\cdot 661$
$(1)(2\cdot 3\cdot 11)(2^2\cdot 5^2)$	$(a)\ 2^0(2-1)\cdot 67^0(67-1)\cdot 5^2(5-1)$	$2\cdot 67\cdot 5^3$
	$(b)\ 2^0(2-1)\cdot 67^0(67-1)\cdot 101^0(101-1)$	$2\cdot 67\cdot 101$
$(1)(2\cdot 5\cdot 11)(2^2\cdot 3\cdot 5)$	$2^0(2-1)\cdot 11(11-1)\cdot 61^0(61-1)$	$2\cdot 11^2\cdot 61$
$(2)(2\cdot 5)(2\cdot 3\cdot 5\cdot 11)$	$(a)\ 3^0\cdot(3-1)\cdot 11^0\cdot(11-1)\cdot 331^0(331-1)$	$3\cdot 11\cdot 331$
	$(b)\ 2(2-1)\cdot 11^0(11-1)\cdot 331^0(331-1)$	$2^2\cdot 11\cdot 331$

表 100 能使 $\phi(N)=2^3\cdot 3\cdot 5^2\cdot 11$ 的 N 值

① 这些带 * 号的因子应予排除，因 A 列与 B 列都出现空缺记号. ——原注.

$\phi(N)=b$ 作为 f_i 的乘积	取公式B形式的 $\phi(N)=b$（Ⅰ的解答）	N（Ⅰ的解答）
$(2)(2\cdot11)(2\cdot3\cdot5^2)$	(a) $3^0\cdot2\cdot23^0\cdot22\cdot151^0\cdot150$	$3\cdot23\cdot151$
	(b) $2\cdot1\cdot23^0\cdot22\cdot151^0\cdot150$	$2^2\cdot23\cdot151$
$(2)(2\cdot3\cdot5)(2\cdot5\cdot11)$	(a) $3^0(3-1)\cdot31^0(31-1)\cdot11(11-1)$	$3\cdot31\cdot11^2$
	(b) $2(2-1)\cdot31^0(31-1)\cdot11(11-1)$	$2^2\cdot31\cdot11^2$
$(2\cdot5)(2\cdot11)(2\cdot3\cdot5)$	$11^0(11-1)\cdot23^0(23-1)\cdot31^0(31-1)$	$11\cdot23\cdot31$
$(1)(2)(2\cdot5)(2\cdot3\cdot5\cdot11)$	$2^0\cdot1\cdot3^0\cdot2\cdot11^0\cdot10\cdot331^0\cdot330$	$2\cdot3\cdot11\cdot331$
$(1)(2)(2\cdot11)(2\cdot3\cdot5^2)$	$2^0\cdot1\cdot3^0\cdot2\cdot23^0\cdot22\cdot151^0\cdot150$	$2\cdot3\cdot23\cdot151$
$(1)(2)(2\cdot3\cdot5)(2\cdot5\cdot11)$	$2^0\cdot1\cdot3^0\cdot2\cdot31^0\cdot30\cdot11\cdot10$	$2\cdot3\cdot31\cdot11^2$
$(1)(2\cdot5)(2\cdot11)(2\cdot3\cdot5)$	$2^0\cdot1\cdot11^0\cdot10\cdot23^0\cdot22\cdot31^0\cdot30$	$2\cdot11\cdot23\cdot31$

表 100　能使 $\phi(N)=2^3\cdot3\cdot5^2\cdot11$ 的 N 值(续)

第91页

Ⅰ. 对 $\phi(N)=b$,某些 b 值不可能有解的情况:对一个奇数 q,若 $2q+1,2^2q+1,2^3q+1,\cdots,2^nq+1$ 全都是合数,且 q 不是 $2^{2^r}+1$ 形式的数(2^r 不超过 n),则 $\phi(N)=2^nq$ 不可能有解. 如取 $q=19,n=5$;则 39;77;153;305;609 统统都是合数,而且 19 又不是 $2^{2^r}+1$ 形式的数;因此 $2\cdot19=38$;$2^2\cdot19=76$;$2^3\cdot19=152$;$2^4\cdot19=304$;$2^5\cdot19=608$ 都是无解的 $\phi(N)$值.

另外还有(1)若 p,q 是奇数,不都是 3 的乘幂,(2)$2pq+1$ 不是素数,(3)q 不等于 $2p+1$,则 $\phi(N)=2pq$ 无解. 例如,$p=3$,$q=15$ 满足了以上各条件,所以 $\phi(N)=90$ 无解. 对 $p=5,q=17$,情况亦然,故 $\phi(N)=170$ 也没有解.

第91页

(a) $\phi(N)=72$ 有 17 解,它们是:73;91;95;111;117;135;146;148;152;182;190;216;222;228;234;252;270.

(b) $\phi(N)=144$ 有 21 解,它们是:185;219;273;285;292;296;304;315;364;370;380;432;438;444;456;468;504;540;546;570;630.

[311]

(c) $\phi(N)=480$ 有 37 解,它们是:527;533;715;723;861;915;964;975;976;992;1054;1066;1144;1148;1155;1220;

1232；1240；1300；1400；1430；1446；1464；1476；1488；1540；1584；1716；1722；1800；1830；1848；1860；1950；1980；2100；2310.

(d) $\phi(N)=2^3\cdot3\cdot5^2\cdot11=6600$ 有 24 解，它们是：$3\cdot3301$；$2^2\cdot3301$；$5^2\cdot331$；$11\cdot661$；$67\cdot5^3$；$67\cdot101$；$11^2\cdot61$；$2\cdot3\cdot3301$；$2\cdot11\cdot661$；$2\cdot5^2\cdot331$；$2\cdot67\cdot101$；$2\cdot67\cdot5^3$；$2\cdot11^2\cdot61$；$2^2\cdot11\cdot331$；$3\cdot11\cdot331$；$3\cdot23\cdot151$；$2^2\cdot23\cdot151$；$3\cdot11^2\cdot31$；$2^2\cdot11^2\cdot31$；$11\cdot23\cdot31$；$2\cdot3\cdot11\cdot331$；$2\cdot3\cdot23\cdot151$；$2\cdot3\cdot11^2\cdot31$；$2\cdot11\cdot23\cdot31$(参看表 100).

(e) $\phi(N)=1$ 的解有两个：$N=1$ 与 $N=2$.

第 91 页

$\phi(N)=b$	解 N	解的个数
1	1;2	2
2	3;4;6	3
4	5;8;10;12	4
6	7;9;14;18	4
8	15;16;20 24;30	5
10	11;22	2
12	13;21;26 28;36;42	6
16	17;32;34 40;48;60	6
18	19;27;38;54	4
20	25;33;44 50;66	5
22	23;46	2
24	35;39;45;52 56;70;72;78 84;90	10
28	29;58	2
30	31;62	2
32	51;64;68;80 96;102;120	7
36	37;57;63;74 76;108;114;126	8
40	41;55;75 82;88;100 110;132;150	9
42	43;49;86;98	4
44	69;92;138	3
46	47;94	2
48	65;104;105;112 130;140;144;156 168;180;210	11

表 101 不大于 50 的一切 $b=\phi(N)$ 所对应的 N 值

第14章的问题

第109页

7. 第328—329页的表103给出了两直角边长只相差1的前100个毕氏三角形的斜边与较短直角边之长.

9. 三边为1357;1476;2005的本原毕氏三角形的周长为4838,面积为1001466.

10. 每边之长在2000与3000之间的本原毕氏三角形为2059;2100;2941.

[312]

第132页

有着同样周长的四个本原毕氏三角形共有以下六个解答,其中,m,n为母数.三边分别为$m^2-n^2, 2mn, m^2+n^2$;周长是$2m(m+n)$.

编号	周长	1		2		3		4	
	$p=2m(m+n)$	m	n	m	n	m	n	m	n
1	543660	390	307	410	253	442	173	510	23
2	554268	374	367	418	245	442	185	494	67
3	570180	390	341	430	233	442	203	510	49
4	570570	385	356	399	316	429	236	455	172
5	949620	490	479	510	421	570	263	646	89
6	986700	506	469	550	347	598	227	650	109

第15章的问题

第145页

数

$$5580731520 = 74088^2 + 9576^2 = 65016^2 + 36792^2$$
$$= 58968^2 + 45864^2 = 72072^2 + 19656^2.$$

第154页

每个人用去的钱是个平方数,而每位丈夫比其妻子要多用去63元,故可列式如下:$M^2-W^2=63=(M+W)(M-W)=$

$63 \cdot 1 = 21 \cdot 3 = 9 \cdot 7$. 由此解出 M,W,可知男人买了 32,12,8 头猪,他们的妻子买了 31,9,1 头猪. 从而可知亨利必定买猪 32 头,因他要比凯塞林多买 23 头,而另外两个买猪数 12 与 8 均小于 23. 由此也可推出凯塞林买的猪必定是 9 头. 采用类似的推理办法,可以判明埃利买了 12 头. 盖特路德买了 1 头. 留下的 8 头猪,肯定是康纳里斯所买,而 31 是安娜买的猪数. 由此可知三对夫妻是亨利—安娜,埃利—凯塞林,康纳里斯—盖特路德.

第 154 页

每位母亲都比她的女儿多消费 4.05 美元,而每人所用去的钱数都是平方数,故可列出式子:$M^2 - D^2 = 405 = (M+D)(M-D) = 405 \cdot 1 = 135 \cdot 3 = 81 \cdot 5 = 45 \cdot 9 = 27 \cdot 15$. 求出五组可能的 M,D 值,并用表格列举出结果以及对应的平方数,于是有:

所买的码数		付出的钱数	
母亲所买 $=M$	女儿所买 $=D$	母亲所付 $=M^2$	女儿所付 $=D^2$
203	202	$412.09	$408.04
69	66	47.61	43.56
43	38	18.49	14.44
27	18	7.29	3.24
21	6	4.41	0.36

[313]

问题的条件终于澄清了事实:女儿的姓氏肯定是艾达·史密斯,安娜·布朗,埃米莉·琼斯,玛丽·鲁宾逊,贝茜·伊文思.

第 157 页

公差为 23,且能形成等差级数的三个平方数,请参看第 317 页,第 25 章问题 21(c)的解答.

第 159 页

边长为 18,15,14,10,9,8,7,4,1 的九个正方形可以组装成一个 33×32 的矩形,见图 25 所示.

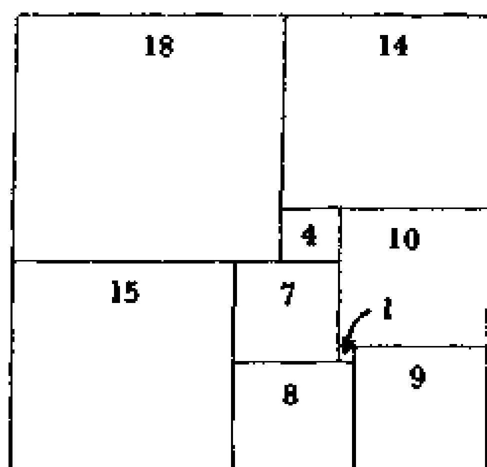


图 25 九个正方形组装成的矩形

第161页

一个 13×13 的正方形可分解为以下各正方形：

$$1\cdot7^2+2\cdot6^2+1\cdot4^2+2\cdot3^2+3\cdot2^2+2\cdot1^2=169.$$

式中各系数之和 1+2+1+2+3+2=11 是此种分解所需的为数最少的正方形的个数，见图 26.

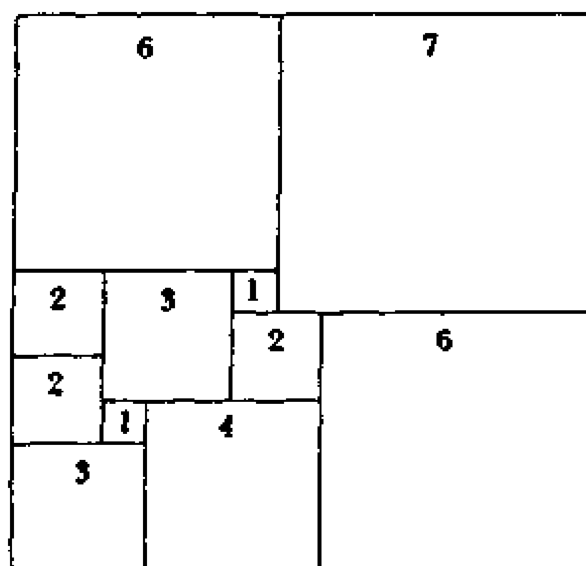


图 26 十一个正方形重新组装成一个正方形 [314]

第19章的问题

第203页

二次同余式 $x^2 \equiv 29 \mod 1193$ 的解是

$$x \equiv \pm 534 \mod 1193.$$

第21章的问题

第233页

各数的因子分解如下：

(a) $23449 = 131 \cdot 179$，

(b) $394831 = 67 \cdot 71 \cdot 83$，

(c) $16503593 = 3733 \cdot 4421$，

(d) $18000001 = 3307 \cdot 5443$.

第22章的问题

第248页

不定方程 $x^2 - 61y^2 = 1$ 的最小解是

$$1766319049^2 - 61 \cdot 226153980^2 = 1.$$

如包括哈罗德自己在内，这支部队应有

$$x^2 = 3119882982860264401$$

人. 如把领袖算进去，这支部队可以排成61个方阵，每一方阵将有$(x^2-1)/61$，即51145622669840400人，也就是226153980的平方. 如果每人占地1平方英尺，则至少要有地球直径三倍大的一个球，才能容纳得下这支部队.

第259页

佩尔方程 $x^2 - 211y^2 = 1$ 的最小解是

$$278354373650^2 - 19162705353^2 = 1.$$ ①

第25章的问题

第294－305页

1. $10.21.

2. 以下各数既是正方形数，又是一个、二个与三个三角形数之和.

正方形数	正方形边长	一个三角形的边长	二个三角形的边长	三个三角形的边长
36	6	8	6;5	5;5;3
1225	35	49	35;34	33;32;16
41616	204	288	204;203	192;192;95
1413721	1189	1681	1189;1188	1121;1120;560
48024900	6930	9800	6930;6929	6533;6533;3267
1631432881	40391	57121	40391,40390	38081;38080;19040

第一年省下36美元，第六年竟然要她省下十六亿三千多万美元！

3. 边长为31、41、49英寸的正方形.

4. 772下，如把开始时的一记敲钟声算进去的话；若不算，那便是771下了.

5. $x=2ab+1$；$y=ab^2-a+b$；$z=ab^2+a+b$.

6. $12\cdot12=144=2\cdot6^2+3\cdot4^2+6\cdot2^2$.

7. 一般说 $1^3+2^3+3^3+\cdots+n^3=n^2(n+1)^2/4$，所以从1开始的连续立方数之和恒为一平方数. 除去1不算，则 $23^3+24^3+25^3=204^2$ 是最小的能给出平方数的连续立方数之和. 但这里的立方数只有三个，而题目却要求三个以上. 五个连续立方数之和 $25^3+26^3+27^3+28^3+29^3=315^2$ 能满足题目条件，但最小的和数是由12个连续立方数相加而得的：

① 此结果有误，遗漏了系数211. —— 译者注.

$$14^3+15^3+16^3+\cdots+25^3=312^2.$$

8. 斜边 $Z=(p^2+q^2)^2$. 直角边长 $X=(p^2-q^2)^2-(2pq)^2$；$Y=4pq(p^2-q^2)$.

9. 只有以下三种方式可以交换：

(a) 一对金刚石耳环调换两颗其他金刚石.

(b) 一对金刚石耳环调换一颗金刚石和一颗红宝石.

(c) 一对红宝石耳环调换两颗金刚石.

就以上情况，珠宝的最小重量如下：

(a) 一对 5 克拉的金刚石耳环调换一颗 7 克拉与一颗 1 克拉的金刚石.

(b) 一对 3 克拉的金刚石耳环调换一颗 4 克拉的金刚石，一颗 1 克拉的红宝石.

(c) 一对 5 克拉红宝石耳环调换一颗 14 克拉金刚石与一颗 48 克拉金刚石.(另一个解是用 40 克拉与 30 克拉金刚石各一颗去调换一对 5 克拉红宝石耳环. 但前一解得出的宝石重量较小.)

(d) 三对耳环的价值分别是 \$50000；\$18000；\$2500000；与之进行交换的宝石价值分别是 \$49000 与 \$1000；\$16000 与 \$2000；\$196000 与 \$2304000. [316]

以下三种情况是不可能进行交换的：

(a) 一对金刚石耳环调换两颗红宝石.

(b) 一对红宝石耳环调换一颗金刚石与一颗红宝石.

(c) 一对红宝石耳环调换两颗红宝石.

这不是一个简单问题.

10. 共有 3 头牛，8 头猪，109 头羊.

11. 三条边应是 $b^2(4a^2-b^2)$，$4a^2(b^2-2a^2)$，$(8a^4-4a^2b^2+b^4)$. 此处 b 为奇数、小于 $2a$ 而大于 $a\sqrt{2}$. 当 $a=2,b=3$ 时所得出的三边 63；16；65 满足题意.

12. 在100000以下的最大平方数是$99856=316^2$,所以,包括将军在内,共有99857人.原先排成两个方阵,其人数分别为$3136=56^2$与$96721=311^2$.

13. 20加仑的那一桶.

14. 最小数:102347586;最大数:987652413.

15. 68.

16. 十位数为3的末两位平方尾数只有唯一的一种可能:36,所以它必然就是本问题中平方数的尾数了.从算式的布局可知,被开方数的最左两位必为10,所以平方根的首位数必定是3.布局又表明根的第二位数字是1.巴罗的平方数表告诉我们,在3100与3200之间,以36结尾的平方数只有一个,即$3194^2=10201636$.当然,本问题不必依赖平方数表,求解并不困难.

17. 除数179;余数164.

18. 12;16;60;144;320;588;1936.

19. 1美元钞票5张,2美元钞票50张,5美元钞票19张.

20. 25.不论他送走24粒还是得到24粒,他拥有的弹子数始终是个平方数.关于三个平方数能组成等差数列的一般公式,在本书第15章中已经给出.

21. (a) 边长恰为11.3;33.7;46.3英寸的正方板.

(b) 80929/1615;106921/1615;127729/1615英寸的方板.

(c) 1140299183/12051130; 905141617/12051130; 581618833/12051130英寸的方板.

本题的一般解虽然存在,但解起来相当困难.

设按照递降顺序的三个平方数是$(Z/Y)^2$,$(X/Y)^2$,$(W/Y)^2$,而公差为A,则有$X^2+AY^2=Z^2$,$X^2-AY^2=W^2$.为了求解起见,应首先找到辅助方程$x^2+y^2=az^2$与$x^2-y^2=bw^2$(其中$ab=A$)的解.从而$X=x^4+y^4$,$Y=2xyzw$.当$A=23$时,辅助方程变成$x^2+y^2=z^2$,$x^2-y^2=23w^2$.后面第二个方程的一般解是

$x=m^2+23n^2$；$y=m^2-23n^2$；$w=2mn$. 将它们代入第一个辅助
[317] 方程，可得出 $2(m^4+23^2n^4)=z^2$. 如令 $n=1$，则 $m=17$ 这个数值将可使表达式为一平方数，这是由于 $2(17^4+23^2)=410^2$ 之故. 于是 $x=312$，$y=266$，$w=34$，$z=410$. 这些数目字中，有公因数 2 可约去，从而给出 $156^2+133^2=205^2$；$156^2-133^2=23\cdot17^2$ 以作为辅助方程的解. 然后，$X=156^4+133^4=905141617$，$Y=2\cdot156\cdot133\cdot205\cdot17=144613560$，$Z=1140299183$，$W=581618833$.

这些解答给出了方板的英尺数；若答数以英寸数表示，则边长在数值上应再乘以 12. 为此，答案中的分数，其分母 Y 应等于 144613560 的 $\frac{1}{12}$，也就是 12051130.

应用类似的办法可解决问题 21a 与 21b.

22. (a) 386 枚；另外两只箱子里装着 8450 与 16514 枚，总数为 25350 枚；

(b) 总数 10086 枚. 三只箱子里分别有 482 枚；3362 枚；6242 枚.

23. 如果他住在这条街的单号一侧，则他家的门牌是 239 号，最后一家的门牌号码为 337；若他住在双号一侧，则他家门牌为 408 号，最后一个号码是 576. 若门牌采取连续编法，则他家是 204 号，最后一家是 288 号. 在以上三种情况下，直到他家为止，但不包括他家门牌号数在内的各门牌号数之和分别为 14161；41412；20706.

24. 比尔的那包脏衣服中有 12 件棉衬衫，6 件尼龙衬衫，洗衣费为 4.68 美元；洗衣费单价如下：每件棉衬衫 24 美分，每件尼龙衬衫 30 美分.

25. 1940 年时他是 55 岁，他死于 1950 年，享年 65 岁.

26. 11236.

27. 有两解：ABC 为 315 或 862. 公因子是 547.

28. 2256 根标准轨.

29. 9.50 或 19.00 美元,要看它是啤酒还是酒.

30. 1936 年 3 月 17 日,星期二. 1908 年 3 月 17 日,星期二是另一个可能的解. 但这位乡下情郎就谈不上年轻了. 1964 年与将近本世纪之末的 1992 年也符合题意.

31. 汤姆以 15 对 1 的赔率投下赌注 15 美元,他赢了 225 美元,加上他原有的 25 美元钱,总数是 250 美元. 比尔以 10 对 1 的赔率投下赌注 10 美元,连同他原有的 25 美元钱共计 125 美元,所以最后他手头的钱数正好等于汤姆的一半. 本问题的求解要涉及佩尔方程,也存在着其他答案,但赔率太大,脱离实际.

32. 三个姑娘和三个小子,每人都拿到一只半个铜板的小面包,以及两只单价是$\frac{1}{3}$只铜板的小面包. 只有一男一女两个似乎也符合条件,但买法将有 10 种,而不是问题所规定的独一无二的买法.

33. 11 英亩.

34. (a) $161^2-1620\cdot 4^2=1$.

(b) $2449^2-1666\cdot 60^2=1$.

[318]

35. 买 4 块樱桃糖,16 块果汁糖. 然后每个孩子分到 1 块樱桃糖,4 块果汁糖. 3 块樱桃糖,2 块果汁糖,15 块杏仁糖的总价也是 40 美分,但无法均匀分配.

36. 此人在 1 个法郎的赌博中连输七次;其后在 7 个法郎的赌博中输了三次,赢了四次;接着在 49 法郎的赌博中输五场,赢二场;然后在 343 法郎的赌博中连赢七场;其后,在 16807 法郎的赌赛中输五赢二;最后在 117649 法郎的赌赛中又连赢七次. 总之,他一共赢得 869288 法郎,输掉 91511 法郎,净得 777777 法郎. 他赢过 26 次,输了 23 次. 本问题实际上是把 777777 表示为 7 的乘幂之和,而其系数均为奇数. 然后,正的系数表示赢的次数,而负的系数表示输的次数.

37. 原来的两堆分别有 120 与 560 颗椰子,其中的三角形底共有 36 与 105 颗椰子,而三角形的每边有着 8 与 14 颗.最后合并成的三棱锥则共有 680 颗椰子,其底座的椰子数为 120,而每边有 15 颗椰子.

38. 若题中并未明确指出此人的硬币数必须多于 100,那么 100 正好能满足题意,因为 $10^2-19\cdot1^2=81$. 在方程 $x^2-19y^2=81$ 中,x 的下一个可能值为 66,因此他至少要有 $66^2=4356$ 枚硬币.而在较小的 19 堆中,每堆应有 $15^2=225$ 枚硬币.第三个可能的解答为 $105^2=11025$ 枚硬币,而 19 堆中的每一堆应有 $24^2=576$ 枚硬币.下列公式可提供无限多组解答:

$$x=10\left[\frac{(170+39\sqrt{19})^n+(170-39\sqrt{19})^n}{2}\right]$$

$$\pm19\left[\frac{(170+39\sqrt{19})^n-(170-39\sqrt{19})^n}{2\sqrt{19}}\right],$$

$$y=\left[\frac{(170+39\sqrt{19})^n+(170-39\sqrt{19})^n}{2}\right]$$

$$\pm10\left[\frac{(170+39\sqrt{19})^n-(170-39\sqrt{19})^n}{2\sqrt{19}}\right].$$

解答当然总是整数;因为表达式中的根式互相抵消了.

不幸的是,上述表达式并不能得出一切可能解,甚至也得不出最小解. $n=1$ 时,得出的两个解是:$959^2-19\cdot220^2=81$, $2441^2-19\cdot560^2=81$.

39. 每种票面的硬币他至少要有 60 枚,其总值为 2100 美元.本问题的其他可能解答是 60 与 2100 的整倍数.

40. 级数至少有 201 级.一般解为 $210k+201$,这里的 k 是任意正整数或零.

41. 99 元 9 角 8 分(美元).

42. 有圆孔的铜钱 7 枚,方孔铜钱 1 枚.

[319] 43. 3651.

44. 对三棱锥而言,三角形底面的一边上放置193只蛋,整个底面有蛋18721只,共193层,总数是1216865只蛋.

如果是四棱锥,底的一边放蛋193只,则正方形底面共有蛋$193^2=37249$只,蛋的总数将是2415009,正好能被最下层支持,这时底层的37249只蛋将受到7.979磅的压力——离极限不远,已岌岌可危.若再加一层的话,那时底的每边将有194只蛋,底面蛋数将是$194^2=37636$,而总数将达2452645.此时底面37636只蛋的每一只要受到8.0209磅压力——那就会顶不住而垮下来,把蛋压扁,搞得一塌糊涂.

45. 边长可为与3,4,5成比例的任何正整数.

46. 15个小正方形.可用$1\cdot6^2+4\cdot3^2+3\cdot2^2+2\cdot4^2+1\cdot5^2+3\cdot1^2$拼成一个$12\times12$正方形,再加上另外单独的一个$5\times5$正方形,见图27.图28则是分成22个正方形的解法.另一个解法也是利用22块,即$1\cdot8^2+4\cdot4^2+16\cdot1^2+1\cdot5^2$,但此处没有给出图解.

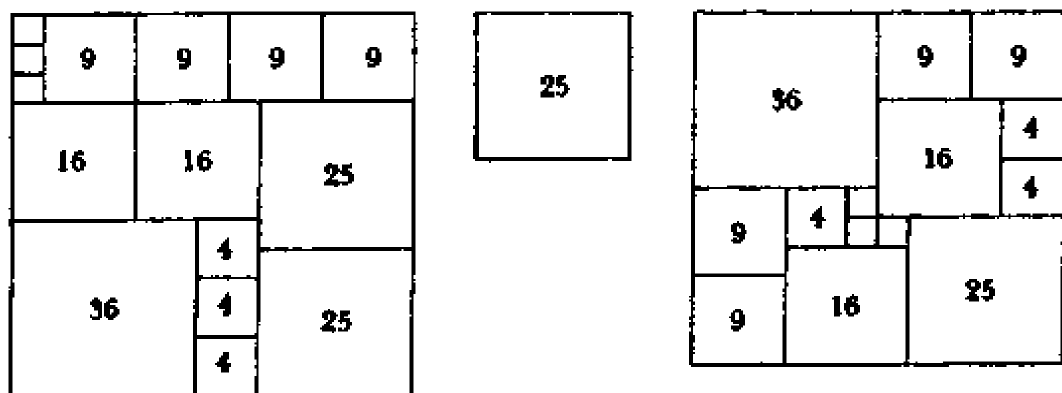
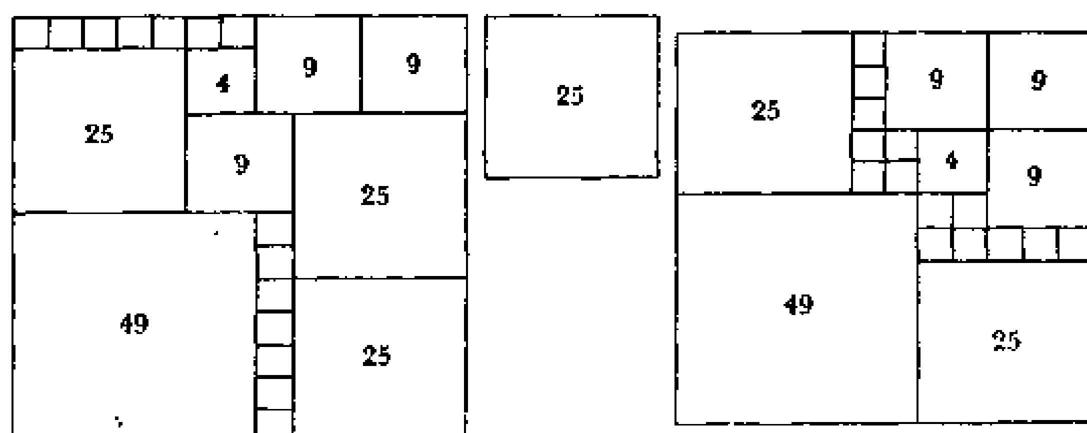


图 27　把一个13×13正方形重组为两个正方形

47. 要求证明$(a^3-1)a^3(a^3+1)\equiv0 \mod 2^3\cdot3^2\cdot7$.

由费马的一般定理可知$a^6-1\equiv0 \mod 3^2$,另由小定理可知$a^6-1\equiv0 \mod 7$.若a为偶数,则a^3能为8整除;若a为奇数,则a^3-1,a^3+1均是偶数,故其中的一个数能被4整除,另一个数能被2整除,于是其乘积能被8整除.又因2^3,3^2,7均彼



[320] 图 28 把一个 13×13 正方形重组为两个正方形

此互质，故 $a^3(a^6-1)\equiv 0 \mod 2^3\cdot 3^2\cdot 7$.

48. 问题 48 的解答由表 102 给出.

$\phi(N)$	N	$\phi(N)$	N
1	1,2	24	35,39,45,52,56,70,72,78,84,90
2	3,4,6	28	29,58
4	5,8,10,12	30	31,62
6	7,9,14,18	32	51,64,68,80,96
8	15;16,20,24,30	36	37,57,63,74,76
10	11,22	40	41,55,75,82,88,100
12	13;21,26,28,36,42	42	43,49,86,98
16	17,32,34,40,48,60	44	69,92
18	19,27,38,54	46	47,94
20	25,33,44,50,66	60	61,77,93,99
22	23,46	72	73,91,95

表 102 具有同一 $\phi(N)$ 的 N 值

49. 1 与 2；3 与 2^2；5 与 2^3；7 与 3^2；17 与 2^5；19 与 3^3；43 与 7^2.

50. 大桶边长为 108 英寸. 由于

$$108^3=104^3+51^3+13^3=106^3+38^3+24^3=96^3+72^3+12^3$$
$$=90^3+72^3+54^3=89^3+82^3+15^3,$$

故知较小的容器，其边长的英寸数分别是 106，104，96，90，89，

82,72,72,54,51,38,24,15,13,12.

51. 设原数为 $N=7K+3$. 若末位的3移到第一位，则形成的新数将是 $3\cdot 7^x+K$（基数为7）. 于是有

$$\frac{4}{5}(7K+3)=3\cdot 7^x+K.$$

化简后可得 $15\cdot 7^x-12=23K$，即 $-8\cdot 7^x\equiv 12 \mod 23$. 由此得出 $7^x\equiv 10 \mod 23$，$x\equiv 21 \mod 22$. 为了得出一个40位以下的解，可取 $x=21$. 于是 $K=(15\cdot 7^{21}-12)/23$，而

$$N=7K+3=[(15\cdot 7^{22}-84)/23]+3$$
$$=15(7^{22}-1)/23.$$

此处的答数是用通常的十进位制表达的，把它写出来，就是 2549883292554122640. 在七进位制中它等于

4364604155323020625113. [321]

若把末位3移到首位，即得 3436460415532302062511，这是原数的 $\frac{4}{5}$（用七进制计算）.

52. 把1000000化为七进制数，算式如下：

除数	被除数	余数
7	1000000	
7	142857	1
7	20408	1
7	2915	3
7	416	3
7	59	3
7	8	3
7	1	1
7	0	1

即 $1000000=7^7+7^6+3\cdot 7^5+3\cdot 7^4+3\cdot 7^3+3\cdot 7^2+7+1$. 百万富翁可以把他的钱作如下分配：

$$
\begin{aligned}
7^7 \text{ 赠款一份} &= \$\,823543 \\
7^6 \text{ 赠款一份} &= 117649 \\
7^5 \text{ 赠款三份} &= 50421 \\
7^4 \text{ 赠款三份} &= 7203 \\
7^3 \text{ 赠款三份} &= 1029 \\
7^2 \text{ 赠款三份} &= 147 \\
7 \text{ 元赠款一份} &= 7 \\
1 \text{ 元赠款一份} &= 1 \\
\hline
&\$\,1000000
\end{aligned}
$$

53. 设 x 为椰子总数. 为了简便起见,可令:

$(n-1)/n=A$,从而有 $A-1=-1/n$,即 $1/(A-1)=-n$.

第一人留下的椰子数为 $A(x-1)$,

第二人留下 $A[A(x-1)-1]=A^2(x-1)-A$,

第三人留下 $A[A^2(x-1)-A-1]=A^3(x-1)-A^2-A$,

……

第 n 人留下

$$
\begin{aligned}
&A^n(x-1)-(A^{n-1}+A^{n-2}+\cdots+A) \\
&=A^n(x-1)-(A^n-A)/(A-1) \\
&=A^n[x-1-1/(A-1)]+A/(A-1),
\end{aligned}
$$

而据题意,它是 n 的一个倍数.

将 A 代入,即得:

$$[(n-1)/n]^n(x-1+n)-(n-1)\equiv 0 \mod n,$$

[322]

$$[(x-1+n)/n^n](-1)^n\equiv -1 \mod n.$$

于是 $(x-1+n)/n^n=kn\pm 1$,两重符号($\pm$)的选取是:n 为奇数时用加号;n 为偶数时用减号. 最后,我们有

$$x=n^n(kn\pm 1)-(n-1)=n^n[kn-(-1)^n]-(n-1).$$

只要 x 是非负数,k 可取任何整数值. 为了找出 x 的最小值,可

按 n 的奇、偶，分别令 $k=0$ 与 $k=1$，结果得出 $n^n-(n-1)$ 或 $(n^n-1)(n-1)$. 当 $n=5$ 时，$x=5^5-4=3121$. 而当 $n=4$ 时，$x=(4^4-1)(4-1)=765$.

若有 n 人，r 只猴子，则第 n 人留下的椰子数将是

$$\begin{aligned}&A^n(x-r)-r(A^{n-1}+\cdots+A)\\&=A^n(x-r)-[r(A^n-A)]/(A-1)\\&=A^n[x-r-r/(A-1)]+Ar/(A-1).\end{aligned}$$

于是有

$$(n-1)^n[(x-r+nr)/n^n]-r(n-1)\equiv 0 \mod n.$$
$$[(x-r+nr)/n^n](-1)^n\equiv -r \mod n,$$
$$(x-r+nr)/n^n=kn\pm r$$

亦即

$$x=n^n[kn-r(-1)^n]-r(n-1).$$

最小解仍然相当于 $k=0$ 或 1，分别对应于 n 的奇、偶，在这两种情况下，结果分别是 $x=rn^n-r(n-1)$ 或 $n^n(n-r)-r(n-1)$.

54. 由于各位数字之和要被 3 与 7 除尽，所以数码 3 的使用次数应是 7 的倍数，而数码 7 的使用次数应是 3 的倍数. 由此可知，所求的最小数应有十位，其中三个是 7，而七个是 3. 这些数码无论作出什么排列肯定都能被 3 整除，这是因为：若一个数的各位数字之和能被 3 整除，则这个数本身也能被 3 整除. 所以，要考虑的是：怎样排列十个数码，才能得出可以被 7 除尽的最小数？

由十个 3 写成的数可记为

$$3\cdot 10^9+3\cdot 10^8+\cdots+3\cdot 10^1+3\cdot 10^0.$$

分别将 $3\cdot 10^9$，$3\cdot 10^8$ 等数除以 7，求出其剩余数，可得出下列表格：

指数 n	$3\cdot10^n$ 的模 7 剩余 r
0	3
1	2
2	6
3	4
4	5
5	1
6	3
7	2
8	6
9	4
剩余之和 =	$36\equiv1 \bmod 7$

[323]

从而可知 3333333333 在除以 7 时将留下余数 1. 因此,有三个位置的 3(其相应剩余之和等于 1 或 8 或 15)必须去掉,以使得其余的和数能被 7 整除. 在这些位置上代之以三个形为 $7\cdot10^n$ 的数不会影响可除性,因为 $7\cdot10^n$ 形式的数当然是对模 7 同余于零的. 要使三个剩余之和为 1,8 或 15,我们只能有下面几种选法:

指数 n	剩余 r	剩余之和 Σr
0,1,6	3,2,3	8
0,2,8	3,6,6	15
0,3,5	3,4,1	8
1,3,7	2,4,2	8
1,4,5	2,5,1	8
2,3,4	6,4,5	15

最后一种选法里出现的最大指数 4 显然要比任何其他选法里出现的最大指数为小,所以由它可得出最小解. 因此 $3\cdot10^2$; $3\cdot10^3$; $3\cdot10^4$ 必须去掉,而代之以 7 为系数的 10 的相应乘幂. 由此可见,3333377733 是最小解.

55. 设数码 3 用过 x 次,数码 5 用过 y 次,数码 7 用过 z

次,则 $3x+5y+7z$ 必能被 3,5,7 整除,也就是被 105 整除. 由此可见,如果在方程 $3x+5y+7z=105$ 中,$x+y+z$ 取最小值,则产生的解必为最小解. 由于变量 z 的系数 7 是最大的,因此只要使 z 值尽量取大,即可使 $x+y+z$ 为极小. 现在用 $z=13,12,11,10$ 进行试探. 我们发现有下列三组 x,y,z 值,均能使 $x+y+z$ 取最小值 17,它们是:$x=3,y=1,z=13$;$x=2,y=3,z=12$;$x=1,y=5,z=11$. 由此可见,所求之数至少应有 17 位. 被 3 整除是不成问题的,因为各位数码之和能被 3 整除;若此数的末位数是 5,那它被 5 整除也不成问题.

让我们分别考察以上三组 x,y,z 值,先来看 $x=3,y=1,z=13$. 此种情况,数码 5 只出现一次,当然它应放在最后一位上. 在数 77777777777777775 中,有三个地方的 7 必须代之以 3,以使新数能被 7 整除. 上面这个数,一看就知道对模 7 是同余于 5 的,因而必须找到 $3\cdot 10^n$ 中的三个 3,而其和是对模 7 同余于 2 的. 另外,应当尽量挑选幂次最高的,使它们尽量在最左面取代 7,只有这样才能得到最小解(见下表).

指数 n	$3\cdot 10^n$ 对模 7 的剩余 r	指数 n	$3\cdot 10^n$ 对模 7 的剩余 r
0	3	9	4
1	2	10	5
2	6	11	1
3	4	12	3
4	5	13	2
5	1	14	6
6	3	15	4
7	2	16	5
8	6		

从表中可以看到,两个最大指数所对应的剩余之和 5+4 正好是对模 7 同余于 2 的,可是我们还得有一个剩余(已经说过要有三个),而表中又没有剩余 0,因此我们不能选取两个最高的方幂,对指数 16 与 14 来说,其剩余之和是 $5+6\equiv 4 \mod 7$,因此为了使和同余于 2(模 7),还应选一个剩余 5,而此数可从指 [324]

数 10 获得. 因此, $7 \cdot 10^{16}$, $7 \cdot 10^{14}$, $7 \cdot 10^{10}$ 必须去掉,而代之以相应位置上的 3. 由此而产生的数 37377737777777775 便是一个数码 5、三个数码 3、13 个数码 7 情况下的最小解.

对其他两组 x, y, z 值,也可用类似办法加以讨论,但问题将变得更为复杂一些,因为要使用的数码 5 不止一个,所以仍须使用列表办法并加以综合考虑. 对 $x=2, y=3, z=12$ 而言,我们最后可得出 33577577777777775;对 $x=1, y=5, z=11$ 而言,相应的解是 35555777777777775. 比较一下上面三个数,第二个数 33577577777777775 是最小的,它才是本问题的解.

56. 九个数码的最小公倍数是 2520,所以该数应能被 2520 整除. 显然,末位数必须是 0,这样它才能被 2 与 5 整除. 同样它应被 7 与 8 整除. 如果以上条件均能得到满足,则此数即能被所有九个数码整除,这是由于全部数码和为 45,所以不管这些数码如何排列,该数总是能被 3 与 9 整除.(若此数能被 8 整除,则也能被 4 整除;若它能被 2 与 3 整除,则它必然也能被 6 整除.)若要被 8 整除,则末三位数必须是以下 16 种情况之一:120;320;520;720;920;240;640;840;160;360;560;760;960;280;480;680.

为了寻找最小解,可以假设左面的前四个数码是 1,2,3,4. 如果在此基础上得不出解,那么可以再假定左面三个数码 1,2,3. 由于不准出现重复数码,右面要考虑的就只能是 560;760;960;680 这样几种情况了. 对模 7 来说,数 1234000560;1234000760;1234000960;1234000680 的剩余分别是 2,6,3,3,因此,必须将尚未用过的几个数码作出适当安排,以产生互补剩余 5,1,4,4.

下面的表格给出了第五、六、七位上未用过的数码的相应剩余,这将大大有助于我们选取合适的排列. 表中未出现数码 7,因为它随便可以放在哪里,都不会影响可除性.

[325]

$a \cdot 10^x$ 的模 7 剩余

x	$a=$ 5	6	8	9
3	2	1	6	5
4	6	3	4	1
5	4	2	5	3

对应于第一种情况 1234000560，无解；第二种情况给出两解：1234895760 与 1234958760；第三种情况有一解 1234857960；第四种情况有一解 1234759680. 最后一个解就是最小解.

57. 见本章的表 103.

58. 利用第 15 章的公式 1：

$$(a_1+1)(a_2+1)\cdots(a_n+1)=24.$$

把 24 分别表示为 2,3,4 个因子的乘积，我们有 $24=12\cdot 2;8\cdot 3;6\cdot 4;2\cdot 2\cdot 6;2\cdot 3\cdot 4;2\cdot 2\cdot 2\cdot 3$，其中最后一个给出了第 15 章讲过的数 N 的因子，即 $a_1=2, a_2=a_3=a_4=1$，于是 $N=5^2\cdot 13\cdot 17\cdot 29=160225$ 就是可用 12 种方法表示为两个平方数之和的最小数. 这 12 种不同办法是：400^2+15^2；399^2+32^2；393^2+76^2；392^2+81^2；384^2+113^2；375^2+140^2；360^2+175^2；356^2+183^2；337^2+216^2；329^2+228^2；311^2+252^2；265^2+300^2.

第 15 章的公式 2 给出：$(a_1+1)(a_2+1)\cdots(a_n+1)=25$，把 25 分解为 $25\cdot 1$ 或 $5\cdot 5$，从后一种分解得出的最小指数将是 4,4. 由此而得出的数 $5^4\cdot 13^4$，虽然也能用 12 种办法表示为两个平方和，但它要比 $5^2\cdot 13\cdot 17\cdot 29$ 大得多.

59. 每位继承人收到的款项都是平方数，而同一家庭的三个平方数是成等差数列的. 三组平方数有着同样的公差，可记为 d. 由第 15 章可知，d 必须等于 $4mn(m^2-n^2)$，并应有三组 m,n 值以产生出同样的 d 值. 这三组值是 7,3;7,5;8,7，给出的 d 值是 3360.（注意 $mn[m^2-n^2]$ 是毕氏三角形的面积；为了得出三

编号	较短的直角边	斜边
1	3	5
2	20	29
3	119	169
4	696	985
5	4059	5741
6	23660	33461
7	137903	195025
8	803760	1136689
9	4684659	6625109
10	27304196	38613965
11	159140519	225058681
12	927538920	1311738121
13	5406093003	7645370045
14	31509019100	44560482149
15	183648021599	259717522849
16	1070379110496	1513744654945
17	6238626641379	8822750406821
18	36361380737780	51422757785981
19	211929657785303	299713796309065
20	1235216565974040	1746860020068409
21	7199369738058939	10181446324101389
22	41961001862379596	59341817924539925
23	244566641436218639	345869461223138161
24	1425438846754932240	2015874949414289041
25	8308066439093374803	11749380235262596085
26	48422959787805316580	68480406462161287469
27	282229692287738524679	399133058537705128729
28	1644955193938625831496	2326317944764069484905
29	9587501471344016464299	13558774610046711780701
30	55880053634125472954300	79026329715516201199301
31	325692820333408821261503	460599203683050495415105
32	1898276868366327454614720	2684568892382786771291329
33	11063968389864555906426819	15646814150613670132332869
34	64485533470821007983946196	91196316011299234022705885
35	375849232435061491997250359	531531081917181734003902441
36	2190609861139547943999555960	3097990175491791170000708761
37	12767809934402226172000085403	18056409971033565286000350125
38	74416249745273809088000956460	105240469650709600546001391989
39	433729688537240628356005653359	613386407933224037990008001809
40	2527961881478169961048032963696	3575077977948634627394046618865
41	14734041600331779137932192128819	20837081459758583726374271711381
42	85876287720512504866545119809220	121447410780602867730851583649421
43	500523684722743250061338526726503	707847383223858622658735230185145
44	2917265820615946995501486040549800	4125636888562548868221559797461449
45	17003071238972938722947577716572299	24045973948151434586670623554583549
46	99101161613221685342183980258883996	140150206800346058651802181530039845
47	577603898440357173330156303836731679	816855266853924917324142465625655521
48	3366522229028921354638753842761506080	4760981394323203445293052612223893281
49	19621529475733170954502366752732304803	27749033099085295754434173207717704165
50	114362654625370104372375446673632322740	161733217200188571081311986634082331709
51	666554398276487455279750313289061631639	942650270102046130733437746596776286089

52	388496373503355462730612643306073746709	5494166403412066213319314492946575384425
53	22643228011924840308557008285075363170939	32022360150370483149182449211052675622461
54	131974404336515487224035923277391441558540	186639992498810810681775380773549480752411
55	769203198007168083035658531379273286180303	1087817594842494380941469835430214208491195
56	4483244783706498010989915264998248275523280	6340265576556155474967043831807735770194769
57	26130265504231789982903833058610216366959379	36953775864494438468860791955415200412677137
58	1522883488416842468864330830866483049926232996	215382389810410475338197708100689466705869803
59	8876598239458734913356946654461368083190438599	1255340561797968413580325456648720509822541401
60	5173660596433557901127734909481645449216398600	7316660981177400006023755031791634132229378601
61	30154303748665473715430714792627904612107953003	42644625325266431622582204734101084193553730205
62	175752161096499284391456553846085882223431319420	248551090970421189729469473372814871029093002629
63	1024358667630340232633308608283887388728479963519	14485681920497260706754234635502788141961004285569
64	5970389984388556421131408395095857238460147448461696	8443420432013143050795938339643913980856932710785
65	34798040395682912435817061966858543312156210806659	49211860671581597598021395402360695743160591979147
66	202817642530251932603493976705300021422789816378260	2868277435974764425373327434074520280478106619164061
67	118210901478558882585146798264940585224582687462903	1671754600913277057625973209044760867125479123005225
68	68898362461833201630073868128843434689924706308399160	97436998618421859932145068201940449422747691118867269
69	40156908462314832295459174079041120354323655162932059	56790444570379838341585067712119508786527129590198509
70	234051614527702673609747857661362378636017224669193186	330998967560396844266891899452523007776864009422323765
71	1364152778703901709363026771889133151461779492852227119	1929203360792001227239666329003018537874660926943744081
72	7950865056769570758256841297367343653013460932444169520	11244221197191610519171106074565588219471101552240140721
73	463410375674703437806047461070151486029346185901812790003	65536123822357661887786979118390510778951946386497100245
74	270095360347126365133716293447235479645942454478432570500	381972521736954360807550714635777476454240588766742460749
75	16742311245152877870162503096132613918463085409608782632999	2226299006599368502957517317695274347946491584213957664249
76	9175291386744600346943785544232332871431908791334263227496	12975821517859256656937553191541868611224708916517003524746
77	53477517195952314414766463075780736836745144207036796031979	75628630100556171438867801831554937319401761914888963484221
78	331689811788969286121634992890452082149038956450886517164380	44079595908547777197506925779778755305185862572811377380581
79	1816661353537863402315043494266931757057488594498282306254303	2569147124412310460411747744955171594511713413521980200799265
80	10588278309438211127768625972711138460195892610538807320361440	149740967873883849904954177211933241811765094618559069827415009
81	617130085030914033642967123419998990041178670687345461615914339	87275373509917999482560755526644279276078854297832438783690789
82	3696089772708110209058011648079288255544511309801868562376124596	508678154812119611904869115947932433844708031168435562754729725
83	20961256277515698509837731761337208434382949991742876812634833239	29647935552727998671946653940160950323792169332712780937764687561
84	12216863893800308896844627408723089550733188640652992313433874040	17280083176824678419775054525017769508908307965108250063833395641
85	71218788335050283530083991276204007670018181852175477087868416803	100715705505675270846703673209945866729657678457936718445235686285
86	415081686016601392283659120248505756469363802472339870094378619980	5870141498572269466604469847346562308690377762782512066607580722069
87	2419273357763958070171871930214829731146167232908223743498201304079	3421369193637686409115978235197991718444568898237135680200248646129
88	14100558460567247028747572261040472630407639495420942590896371204496	19941201011966891508035422426453294080038375626640302014593911154705
89	82184077405639524102313561630028004061299669739543431801873935922899	116225836878175662639096556323521772761745684861604878407363218282101
90	4790019059732698975851337974551275636773903789418396482203482441332900	677413820257085084326543915514677342490435733542987756429585398537901
91	27818393584339798614084689223604737374013042603911494457520215630074503	3948257084664334843320166936764542282180868716398321862170149172945305
92	16272032244630609270865801544613296892400865244527127094900944936114120	23012128687728923975594457705072576350594776564834943416691309839183929
93	946403641093496757637863200439850427783921486632512668123885454086616219	134124515041709209010246579290670915821387790672613338637377708661858269
94	522270092411447446311852118719296959977952027934980481644411779583547196	781734861562526330085885018056952918577731987470845088407674942332015685
95	32217802003594549961073263922717987170893200187466316217545852234114872959	4556285254333448771505083529048046595645004014152457191808671945330235841
96	18777911109745262531332104234911483342557968084644809248861099660904490560	265559765644381662989444961562313266552922921174438980624443567729649399361
97	109445686445811212019168531102719710330258408408522223871632012142012270403	154779574132295549022161913408339913336108748690510931182857468432566160325
98	637896207638927458619979759868271136686992962846588533980310973291169131660	902121468229335127834026984293808153361360290025621689034700453865747562569
99	3717931559375452631527893248192429716783499288591008980010333827605002520759	525794923524371521798199992354509006832052451463219203025345254761919215209
100	21669693148613788330547979729286307164015202768699465346081691992338845992696	3064557394323295618009579729698332458876309545096753693529117371074705767728665

表 103 直角边为连续数的毕氏三角形

个等面积的直角三角形，可令 $m_1=m_2=r^2+rs+s^2$，$m_3=r^2+2rs$，$n_1=r^2-s^2$，$n_2=2rs+s^2$，$n_3=r^2+rs+s^2$. 令 $r=2$，$s=1$，即可得出三组数值：7，3；7，5；8，7.）把三组 m，n 值代入构成等差数列的三平方数：

$$X=m^2-n^2-2mn;Y=m^2+n^2;Z=m^2-n^2+2mn;$$

[326] 即可得出相应的三个三数组：

Z^2（丈夫）	Y^2（妻子）	X^2（孩子）	和
$6724=82^2$	$3364=58^2$	$4=2^2$	\$ 10092
$8836=94^2$	$5476=74^2$	$2116=46^2$	16428
$16129=127^2$	$12769=113^2$	$9409=97^2$	38307
		合计	\$ 64827

第一列的钱数属于丈夫，第二、三列则分别属于妻子与孩子. 因为一共只有四个女性，所以孩子们必定是一个女儿，两个儿子. 考虑这些因素再结合问题的其他条件，我们发现 $5476+3364=8836+4=8840$，$8836+5476+2116=16129+299=16428$. 琼斯家得到的钱要比布朗家多三分之一，所以琼斯家所得的款数肯定是第二行数字，而布朗家的得款数是第一行数字. 这样就完全确定了三个家庭中每个成员的身份及其接受的遗产：

比尔·琼斯	\$ 8836	亨克·史密斯	\$ 16129	杰克·布朗	\$ 6724
玛丽·琼斯	5476	爱莉莎·史密斯	12769	莎拉·布朗	3364
奈特·琼斯	2116	苏珊·史密斯	9409	汤姆·布朗	4
	\$ 16428		\$ 38307		\$ 10092

60. 若不算个位数 D，由其他数码所成之数为 A，则此数是 $N=10A+D$，而 $D\cdot10^x+A$ 是新数，其中 x 表示 A 中数码的个数. 由此可知，N 有 $x+1$ 位，而 $K(10A+D)=D\cdot10^x+A$，即 $A(10K-1)=D(10^x-K)$. 所以 $A=D(10^x-K)/(10K-1)$. 由于 $N=10A+D$，故得

$$N=D(10^x-1)/(10K-1),$$

这里,$e=x+1$. 对给定的 K 来说,N 的最小值有 e 位数码.

下面的表格给出了一些 K 值,以及当 D 与 $10K-1$ 互质时,N 中可能有的最少位数 e.

K	$10K-1$	e
2	19	18
3	29	28
4	39	6
5	49	42
6	59	58
7	69	22
8	79	13
9	89	44
10	99	2

因此,当个位数移至首位时,要将 N 乘以 6,所需的数当不少于 58 位,但要把它乘以 4 则只需要一个 6 位数. 若 $K=2$, [327] $D=2$,则 N 是一个 18 位数 105263157894736842.

对 N 值来说,公式中的分母 $10K-1$ 恒与数码 $D=2,4,5,8$ 互质,故对这四个数码来说,N 中数码的个数与 D 值无关,而只取决于 K 值. 当 D 与 $10K-1$ 不互质时,分母将可约简,也就降低了 e 的数值. 下表将给出 D 与 K 值,为了求出 e 而必需求解的同余式,以及 N 值:

D	$10K-1=$	$10^e-1\equiv 0 \bmod$:	N
3	$3m$	m	$(10^e-1)/m$
6	$3m$	m	$2(10^e-1)/m$
7	$7m$	m	$(10^e-1)/m$
9	$9m$	m	$(10^e-1)/m$
9	$9m\pm 3$	$3m\pm 1$	$3(10^e-1)/(3m\pm 1)$

例如,若 $K=5$,则 $10K-1=49$,$e=42$,对 7 以外的一切 D 值,N 要有 42 位数码. 而对 $D=7$ 来说,N 只要 6 位,它的最小解是 142857. 所以,D 的值对 N 是有相当影响的. 但将模 $10K-1$ 除以 3 或 9 不会降低 e 值,除非 $10K-1$ 含有大于 9 的、3 的方幂,甚至也并非必然. 例如 $K=46$ 将是最小的值,对它来说,

选取 $D=3,6,9$ 将把 e 值从 48 减少到 16,而对另外 5 个数码来说,$e=48$ 是必不可少的. 对一个较小的 K 值,而使 $10K-1$ 能被大于 9 的 3 的乘幂整除时,例如 $K=19$,$10K-1=27\cdot 7$,则不管 D 取什么数值,e 的值都等于 6.

若 $(K-D)>\frac{1}{10}$,则为了得出正确结果,N 必须从 0 开始;如果 $(K-10D)>\frac{1}{10}$,则前面需有两个 0;若 $(K-100D)>\frac{1}{10}$,则前面得有三个 0,……依此类推,例如,若 $D=7$,$K=8$,由于 $8-7=1$,超过了 $\frac{1}{10}$,于是 $N=7(10^{13}-1)/79$ 必须写作 0886075949367,且有 $8N=7088607594936$. 但若 $D=9$,$K=8$,则因 $8-9=-1$ 小于 $\frac{1}{10}$,故而 $N=9(10^{13}-1)/79=1012658227848$ 中不需要在前面加上 0. 若 $D=2$,$K=21$,由于 $21-20>\frac{1}{10}$,因此 $N=2(10^{18}-1)/209$ 必须写成 0095693779904306 22,只有这样写才能有 $21N=2009569377990430 62$.

61. 设支票面额为 $1000x+100y+10z+u$,则误付的款项为 $1000u+100z+10y+x$. 亏损数 $B^2=999u+90z-90y-999x$. 于是

$$111(u-x)+10(z-y)=B^2/9=A^2$$

是另一平方数. 设 $u-x=L$,$z-y=M$. 显然首位数码 x 不可能是 0,L 也不能为 0,否则 $10(z-y)$ 将是一个平方数,但因 $(z-y)<10$,这肯定是不可能的,因此,$0<x<8$,$0<L<9$. M 可正可负,但不能为 0,因若等于 0,则 $111L$ 将是一平方数,但因 $(u-x)<9$,这是不可能的,由此可知 $0<|M|\leqslant 9$. 从而 $111L+10M=A^2$,$M\equiv A^2 \bmod 3$,因而 M 是 3 的平方剩余,即 $\pm(1,3,4,7,9)$. 由于平方数总是以 0,1,4,5,6,9 结尾,而 $10M$ 的尾数

必定是0,因而111L的尾数总是0,1,4,5,6中的一个(因$L<9$). 于是可知$111+10M$, $444+10M$, $555+10M$, $666+10M$必为一平方数. 把这些可能情况用表格列举出来:

解的类型	M	L	$A=\frac{B}{3}$	亏损数 $=B^2$	$z=y+M$	$u=x+L$	范围 x	范围 y	解$=x$与y的组合
1	1	1	11	1089	$y+1$	$x+1$	1—8	0—8	72
2	1	6	26	6084	$y+1$	$x+6$	1—3	0—8	27
3	4	4	22	4356	$y+4$	$x+4$	1—5	0—5	30
4	7	5	25	5625	$y+7$	$x+5$	1—4	0—2	12
5	−3	1	9	729	$y-3$	$x+1$	1—8	3—9	56
6	−9	6	24	5184	0	$x+6$	1—3	9	3
								总计	200

因此,有六个平方数是有可能的,我们已把它们列举在B^2这一列,支票有200种不同金额可开.

第2型解答共有27种,其中有两个可能的解答是\$18.97与\$30.19. 第5型解答有56种,其中有两个解是\$35.24与\$13.02. 其他解答亦可类似地得出,这只要在规定范围内指定x与y值就行.

62. 仿照问题61的解法,我们将有$111L+10M=B^3/9=3A^3$,故$B=3A$,由于$L<9$, $|M|<10$,所以$3A^3<978$,即$A^3<326$. 由于$7^3>326$,所以我们只需考虑1到6的A值就行. 对这些值,只有$A=3$与4有解,分别能得出$L=1$, $M=-3$与$L=2$, $M=-3$. 两个立方亏损数为729与1728. 在第一种情况,$x=1$至8, $y=3$至9, $z=y-3$, $u=x+1$. 对x, y的各种可能组合将给出56个解. 对第二种情况,$x=1$至7, $y=3$至9, $z=y-3$, $u=x+2$. 可给出49个解,两者合计,解答总数是105种. 对两种类型的解答,我们可以各举一例:\$83.09与\$37.45.

63. (a)数N显然能被111整除.

(b) C必定是0,5,8或9,只有这样,当N增加1时才能得到末三位平方尾数.

(c) C不能等于9,否则S^2的末尾将接连出现三个0,但平

方数的末尾 0 的个数应是偶数.由此可知 S^2 必以 001,556 或 889 结尾.

(d) $111222333<S^2<999888777$,或 $10546<S<31621$.

(e) 容易证明,若 S^2 的末三位数与较小的 T^2 的末三位数相同时,则必有以下关系:T 为偶数时,$S^2=(500K\pm T)^2$;T 为奇数时,$S^2=(250K\pm T)^2$①.如取偶数值 556,则具有此种尾数的最小平方数 T^2 将是 $166^2=27556$,代入上述"偶数型公式",我们即可得出有此三位尾数的一切平方数 $S^2=(500K\pm 166)^2$.于是 $(500K\pm 166)^2-1\equiv 0 \mod 111$,$K\equiv\mp 1,\pm 3, \mod 37$(37 [331] 是 111 的一个除数),仅当 $K=34;36;38;40$ 时才能使 S 值落入(d)的范围,可是没有一个 S 值能符合条件.

再考虑奇数尾数 001,此时,最小平方数为 1,代入"奇数型公式",可知 $S^2=(250K\pm 1)^2$ 表示一切具有 001 尾数的平方数.于是有 $(250K\pm 1)^2-1\equiv 0 \mod 111$,即 $K\equiv 0$ 或 $\mp 8, \mod 37$.此时仅当 $K=45;66;74;82;103;111;119$ 时才能使 S 落入(d)所限定的范围,然而,我们的希望再次落空了,仍然是无解.

最后考虑 889,最小平方数 $T^2=83^2=6889$.于是 $S^2=(250K\pm 83)^2$.即 $(250K\pm 83)^2-1\equiv 0 \mod 111$,从而 $K\equiv\mp 3,\pm 5, \mod 37$.仅当 $K=42;69;71;77;79;106;108;114;116$ 时能使 S 落入由(d)限定的范围.通过计算,可知 $K=42$ 时得出 $S=10583$,而 $S^2=111999889$,于是所求之数为 111999888.除此以外,S 的所有其他值都得不出解.

64. 考察从 0 到 10^n-1 的一切正整数.(10^n-1) 含有 n 个 9.我们把 0 与此数配成一对,把 1 与 10^n-2 配对,2 与 10^n-3 配对,如此等等.由于把 0 算进去的话,共有 10^n 个正整数,于是就有 $10^n/2$ 对,但每对之和等于 10^n-1,它们的各位数码之和是

① 设 T 不能被 5 整除.如 T 能被 5 整除,则我们在公式中要用 $50K$ 取代 $250K$,用 $100K$ 取代 $500K$.——原注.

$9n$. 既然一共有 $10^n/2$ 对,因此,所有数码之和是 $9n\cdot 10^n/2$,再把表示 10^n 的数码 1 加上去(其他数码都是 0 了),便得到 $[9n\cdot 10^n/2]+1=45n\cdot 10^{n-1}+1$. 对十亿来说,$n$ 相当于 9,因此这个和数是 4050000001.

65. $3^2\equiv 2 \mod 7$; $3^{2x}\equiv 2^x \mod 7$; $3^{2x+1}\equiv 3\cdot 2^x$. 于是有

$$3^{2x+1}+2^{x+2}\equiv 3\cdot 2^x+2^{x+2}=2^x(3+2^2)=2^x\cdot 7\equiv 0 \mod 7.$$

66. 设 $F=0.TALKTALK\cdots$

则 $10000F=TALK.TALK\cdots$

相减后得 $9999F=TALK.$

于是 $(EVE)/DID=F=(TALK)/9999$. 由此可见 $(TALK)/9999$ 化成最简分数后就等于 $(EVE)/DID$,所以分母"DID"肯定是 9999 的一个三位数因子,即 101,303 或 909.

(a) 设 $DID=101$. 则 $(EVE)/101=(TALK)/9999$,或 $TALK=(EVE)99=(EVE)(100-1)=EVE00-EVE$. 相减以后,首位数仍将是 E,不能是 T,因此 $DID\neq 101$.

(b) 再设 $DID=909$. 则 $(EVE)/909=(TALK)/9999$ 或 $TALK=(EVE)11=(EVE)(10+1)=EVE0+EVE$,可见末位数为 E,不可能是 K. 因此 $DID\neq 909$.

(c)剩下唯一的可能 $DID=303$. 由于 F 是一个真分数,EVE 只能是(1 * 1)或(2 * 2),要试探的数只有 121;141;151;161;171;181;191;以及 212;242;252;262;272;282;292 这几种. 除 242 外,所有其他分子都将在商数中重复出现已经有过的数字. 所以符合条件的只有一个 $242/303=0.79867986\cdots$.[①]

67. 作直线 BG. 由假设可知 $\angle ABF=45°$,于是 $\angle BAE=45°$,因此 $AE=BE$. 斜边上的中点 G 总是与其他三顶点等距的,

---

① 根据本问题的原始提法,只说是普通分数而并未注明必须为最简分数,因而本题尚有另外一解:$\frac{212}{606}=0.\dot{3}49\dot{8}$,它也是符合字母代换原则的. —— 译者注.

$\therefore AG=BG$. G、E 决定了 AB 的垂直平分线，从而 $DG\perp AB$. 于是 $AD=DB=DE$. DG 是三角形中两边中点的联线，从而 $DG=\frac{1}{2}BC$. 由于 ABC 是一个毕氏三角形，可令 $BC=m^2-n^2$，于是 $AB=2mn$，$AD=DE=mn$，而 $mn+49=(m^2-n^2)/2$，即$(m-n)^2-2n^2=98$. 这个不定方程的最小解是 $m-n=10$，$n=1$，$m=11$. 于是 $AB=22$，$BC=120$，$AC=122$.

[332]

如果改取 $BC=2mn$，则 $AB=m^2-n^2$，$DE=(m^2-n^2)/2$ 且有$(m^2-n^2)/2+49=mn$，即$(m-n)^2+98=2n^2$，这个不定方程的最小解是 $m-n=8$，$n=9$，$m=17$. 于是 $AB=208$，$BC=306$，$AC=370$.

68. 设此三位数为 N，其各位数字之和为 S，设 $N\equiv a \bmod 9$，则 $S\equiv a \bmod 9$，这是由于一个数除以 9 时，其余数等于其数字和的九余数. 于是有$(9K+a)/(9L+a)=26$，即 $9(K-26L)=25a$. 而 $a=0,9,18$ 等等，最小值是 0. 故有 $K=26L$，为了求得最小值，可令 $L=1$，此时 $K=26$，$N=234$，$S=9$.

69. 由第 15 章的公式 1 与公式 2，数 N 能表示为两个平方数之和的方法数为

$[(a_1+1)(a_2+1)\cdots(a_n+1)-1]/2$（所有的 a_i 均为偶数）

或

$[(a_1+1)(a_2+1)\cdots(a_n+1)]/2$（至少有一个 a_i 是奇数）.

令以上二式为 7，我们将得到$(a_1+1)(a_2+1)\cdots=15$ 或 14，从而 $a_1=4$，$a_2=2$ 或 $a_1=6$，$a_2=1$. 这些都是用于 $4x+1$ 形式的素数 p 的指数的. 由此得出 $N=5^4\cdot13^2$ 或 $N=5^6\cdot13$，前者为最小数.

由于 $5^4\cdot13^2$ 碰巧是一个平方数，这使找出它的七种平方和分解法较为方便. 只要找出毕氏三角形的七对直角边，以使得 $5^4\cdot13^2$ 为斜边的平方就行. 设这些直角边为 $A=K(x^2-y^2)$，$B=K(2xy)$，于是斜边 C 为 $K(x^2+y^2)=5^2\cdot13=325$，而 $N=$

C^2. 把 325 分解为其因子对 K 与(x^2+y^2),我们就能得到下表中的各个数值:

K	x^2+y^2	x	y	A	B	$C^2=A^2+B^2=N=5^4\cdot 13^2$
65	5	2	1	195	260	105625
25	13	3	2	125	300	105625
13	25	4	3	91	312	105625
5	65	8	1	315	80	105625
5	65	7	4	165	240	105625
1	325	17	6	253	204	105625
1	325	18	1	323	36	105625

第二种类型的解答要用到 $N=5^6\cdot 13=203125$,由于它不是一个平方数,因此不能利用毕氏三角公式,但仍易找到七种分解法:先提出平方因子5^6,5^4,5^2或5^0,再把商分解成两个平方数之和,再把平方因子乘进去.七个解答如下: [333]

$$5^6(2^2+3^2)=250^2+375^2;\quad 5^4(18^2+1^2)=450^2+25^2;$$
$$5^4(17^2+6^2)=425^2+150^2;\quad 5^2(69^2+58^2)=345^2+290^2;$$
$$5^2(86^2+27^2)=430^2+135^2;\quad 5^0(366^2+263^2)=366^2+263^2;$$
$$5^0(439^2+102^2)=439^2+102^2.$$

70. 两个平方数是 $5500002244=74162^2$ 与 $7744000000=88000^2$.

平方数加 7 以后所得之数为 $34641^2+7=1199998888$, $99559^2+7=9911994488$.

71. 设 x 为母牛数,小羔羊的价值是 L. 售牛所得为 x^2 元,由于每人都分到同样头数的动物,其中也包括小羊羔在内,由此可见买进的绵羊数 y 是个奇数. 列式如下:$x^2=10y+L$. 但若一个平方数的倒数第二位是奇数,则最后一位 L 必然等于 6. 因此小羊羔值 6 元,为了交易公平,分到小羊羔的人还应该再收进补偿金 2 元.

72. 设原数为 x^2,增援兵力为 $10y^2$,最后总人数为 $400z^2$. 由题意可列出式子:$x^2+10y^2=400z^2=(20z)^2=w^2$. 由条件

$5,000,000<400z^2<15,000,000$ 即 $158<z<194$,从而 $3160<w<3880$. 从该方程可解得 $x=K(rm^2-sn^2)$; $y=2mn$; $w=K(rm^2+sn^2)$;这里的 K,m,n 可自由选取,但 rs 必须等于 10(y 的系数). 由此可见,存在着无限多组解,例如 $18^2+10\cdot4^2=22^2$ 等等. 在指定的范围内,$K=60,r=5,s=2,m=3,n=2,x=2220,y=720,w=3180,z=159$. 于是有 $2220^2+10\cdot720^2=4,928,400+5,184,000=10,112,400=3180^2=400\cdot159^2$,所以在排成的 400 方队中,每队人数均为 $159^2=25281$.

73. 由于 72 能被 8 整除,所以付出的价款必能被 8 整除,1000 及 10 的更高次幂肯定都能被 8 整除,因此只要考虑 79 * 能被 8 整除就行. 由此即可肯定末位数必定是 2. 火鸡只数能被 9 整除,其价款也应如此,所以各位数码之和亦能被 9 整除. 由此可知第一位数字必定是 3;所以总的价款必定等于 367.92 美元,而每只火鸡的价格是 5.11 美元.

74.
$$85555^2-1=7319658024,$$
$$97777^2-1=9560341728.$$

75. 十个数码齐全,不重不漏的平方数共有 87 个,其中最小的是 $32043^2=1026753849$,最大的是 $99066^2=9814072356$.

76. 若平方根不是回文数,则共有 44 个解答,其分布范围在 35902^2 至 98182^2 之间. 但平方根是回文数的却只有唯一解,即 66266. 此数平方后再减去一百万,即得所求数 4390182756.

[334]

77. 若平方根不是回文数,则共有 26 个解,其范围在 12817^2 至 29024^2 之间. 平方根为回文数的只有一解,即 18181,它的平方再减去一百万,即得 329548761.

78.
$$87695^2=7689413025+10^6,$$
$$23104^2=532794816+10^6.$$

79. 根据题目里头的条件,$H^2=W^2+S^2+D^2$,$F=H^2+W^2+D^2$,故有 $2H^2=S^2-F$,可见儿子的年龄是一奇平方数. 对两个孩子来说,即使是年仅 1 岁的双胞胎,妻子的年龄也应大于

16 岁,因而她至少是 25 岁. 于是夫妻的年龄只能是下列几种情况:36/25,49/25,64/25,49/36,64/36.其他年龄组合将导致老父的年龄超过 109 岁,而这未免是太老了.夫妻年龄之差可为下列几种情况:11,24,39,13,28.其中只有 13 是两个平方数之和 S^2+D^2,而这是必要形式 K^2p,其中 p 是 $4x+1$ 形素数之乘积.于是 $S=3^2$,$D=2^2$,$H=49$,$W=36$,而 $F=49+36+4=89$,是一个素数.妻子的年龄是 36 岁,正好是一个"完善的 36".

80. $N=99991=10^5-9$,这是一个素数.于是有 $10^5\equiv 9$,$10^5+1\equiv 10$,$10^5-1\equiv 8 \mod N$.从而 $10^{10}-1\equiv 80$,$(10^{10}-1)^{99989}\equiv 80^{99989}$,即 $1+(10^{10}-1)^{99989}\equiv 1+80^{99989}$.此外,$10^{999890}=[(10^5)^2]^{99989}\equiv(9^2)^{99989}\equiv 81^{99989}$.故而 $10^{999890}-1\equiv 81^{99989}-1$.于是 $1+80^{99989}=80(1+80^{99989})/80=(80+80^{99990})/80\equiv(80+1)/80 \mod N$;而 $81^{99989}-1=81(81^{99989}-1)/81=(81^{99990}-81)/81\equiv(1-81)/81\equiv-80/81 \mod N$,这是利用了费马定理而得的结果.于是

$$1+[1+(10^{10}-1)^{99989}](10^{999890}-1)$$
$$\equiv 1+(81/80)(-80/81)\equiv 1-1\equiv 0 \mod N.$$

81. 15 是可为五个毕氏三角形之一边的最小整数.这些边是 15-20-25,15-36-39,8-15-17,15-112-113,9-12-15.其相应面积分别为 150,270,60,840,54.它们的总面积是 1374 平方单位.正五边形之面积$=(S^2/4)(25+10\sqrt{5})^{\frac{1}{2}}$.在此种情况下 $S=15$,面积$=(225/4)(25+10\sqrt{5})^{\frac{1}{2}}$平方单位.

82. 本问题中待求之数是两数的除数.为此,需先求出两数的最大公约数,大多数算术或代数课本中都讲过这种求法.本题的最大公约数 887 是个素数,因此每个电子零件价格为 \$8.87,去年共售出 937 个零件.

如果你手头没有现成课本,那也不要紧.用 389393 去除 831119,得商数 2,余数 52333.再用余数去除 389393,得商数 7,

余数 23062. 仿此进行，每次用余数去除前一除数. 能使余数为 0 的第一个除数便是待求的最大公约数.

83. 相似立体的体积之比等于其线性尺度的立方之比，由此可知两球的体积之比是 $1^3/2^3$，即 1/8. 它们合起来的体积因而是 $9K$ 立方英寸，这里的 K 是一个比例常数（$K=1/6\pi^2$），把 [335] 烧瓶周长的立方数转化成体积时必须乘以 K. 于是问题转化为求解 $Kx^3+Ky^3=9K$，即 $x^3+y^3=9$. 满足这个方程的最小值为

$$x = 415280564497/348671682660,$$
$$y = 676702467503/348671682660.$$

这两个分数便是两只烧瓶周长的英尺数.

84. 1111111 的素数因子是 239 与 4649，所以一定是 239 辆汽车，而每辆汽车的售价为 4649 美元.

85. 方程 $x^3+y^3=6$ 的解是 $x=17/21$，$y=37/21$.

86. 可参看第 14 章. 具有相等面积的四个最小毕氏三角形，其边长分别是(111，6160，6161)，(231，2960，2969)，(1320，518，1418)，(280，2442，2458). 每个三角形的面积都等于 341880. 由于边长为 $1\frac{1}{4}$ 英里的方形土地的面积是 43560000 平方英尺，所以，除去角上的 4(341880)＝1367520 之外，农夫还保留着 42192480 平方英尺土地，这个数字超过了原有面积的 96%.

87. 见第 14 章. 具有相等周长的四个最小本原毕氏三角形如下：

(153868，9435，154157)，(99660，86099，131701)，
(43660，133419，140381)，(13260，151811，152389).

88. 数 $N^2=abcdefabc$ 可分解为 $(abc)(1002001)=(abc)\cdot 7^2\cdot 11^2\cdot 13^2$. 但因 $def<1000$，所以 $abc<500$，且必须是一个平方数. 于是其平方根 r 必在 10 与 23 之间，且为一素数. 由此可

知，r 只能是 17 或 19，因为 13 已被用过. 所以 $r^2=(abc)=289$ 或 361，而 $N^2=289578289$ 或 361722361. 因此 $N=7\cdot11\cdot13\cdot17=17017$ 或 $7\cdot11\cdot13\cdot19=19019$.

89. 作为两个平方数之和的整数 N 必须等于 N_0m^2，这里 m^2 是 N 与 N_0 中的最大平方数，且不含有 $4x-1$ 形式的素数因子(见第 15 章). 但任意三个连续数中必有一个数能被 3 整除，而 3 又是 $4x-1$ 形式的素数，因此 3 必须以偶次幂形式出现于一个数中，从而我们应在 9 的倍数中去寻找. 在 27，54，63 中，N_0 含有一个 $4x-1$ 形式的素数；在 9 或 36 中它们不能表示为两个平方数之和. 18 与 45 虽能作如此表达，然而相邻数 16，19 或 44，46 又不行. 再来看一看数 72，它可以表达为两个平方数之和，71 不行，可是 73 与 74 合适；因而 $72=6^2+6^2$；$73=3^2+8^2$；$74=5^2+7^2$. 利用不同素数的最小解(不像 72 那样，用了两个同样的 6)是 $232=6^2+14^2$；$233=8^2+13^2$；$234=3^2+15^2$.

90. 设模糊不清的数码是 x 与 y. 把各位数码相加，其和是 $x+y+30$. 隔位相加，并从一组和数减去另一组和数，可得 $12+x-y$. 若数码和能被 9 整除，则该 8 位数也能被 9 整除；而若 $12+x-y$ 能被 11 整除，则该 8 位数亦然. 于是有 $x+y+z\equiv 0 \mod 9$，$12+x-y\equiv 0 \mod 11$. 有六对数值能满足第一个同余式，但只有 7，8 这一对能满足第二个同余式，因此 $x=7$，$y=8$. 所求的数是 27374985. [336]

91. 设 h=马匹数，c=小鸡数，则有关系式 $h+c+2c=4h+2c$，于是 $c=3h$. 从而小鸡数为马匹数的 3 倍，只要它们的头数为 3 与 1 之比都可满足题意.

92. 知道余数及减数，我们即可写出相应的被减数 2071 与 2622，以及被除数 95221. 然后算出三个减数的最大公约数 345，它就是除数，从而可以算出商数为 276.

93. 在七进位制中，此数可记为 $a\cdot7^2+b\cdot7+c$；在九进位制中，它是 $c\cdot9^2+b\cdot9+a$. 列出等式：$48a=2b+80c$，即 $8(3a-$

$5c)=b$. 但在七进位制中没有数码 8，因此 b 必须等于 0，于是 $3a=5c$，由此得出 $a=5$，$c=3$，这个数在七进位制中是 503，而在九进位制中是 305. 若用普通十进位记法，它是 248.

94. $(x^5/5)+(x^3/3)+(7x/15)=[(x^5-x)/5]+[(x^3-x)/3]+x$. 但由费马定理可知 $x^5-x\equiv 0 \mod 5$，$x^3-x\equiv 0 \mod 3$，因而整个表达式为一整数.

95. 能被 2，3，5 整除的数 N 可记为 $N=2^a3^b5^c$. 由于 $\frac{N}{2}$ 是一平方数，所以 a 必须是奇数，b 与 c 应是偶数. 类似地可推论出 a，c 必须是 3 的倍数，而 $b\equiv 1 \mod 3$. 另外，a，b 应是 5 的倍数，而 $c\equiv 1 \mod 5$. 满足这些条件的最小数是 $a=15$，$b=10$，$c=6$，于是

$$N = 2^{15}\cdot 3^{10}\cdot 5^6 = 30,233,088,000,000.$$

96. 有两解：$300^3-5000^2=2,000,000$；$129^3-383^2=2,000,000$. 方程 $a^3-b^2=2c^2$ 的解法可参看乌思宾斯基与希斯莱特合著的《基础数论》，美国马克格劳希尔图书公司 1939 年版，393—395 页.

97. $p-i\equiv -i \mod p$，因而

$$(p-1)(p-2)\cdots(p-r)\equiv(-1)(-2)\cdots(-r)$$
$$=(-1)^r\cdot r!.$$

在同余式两端各乘以 $(p-r-1)!$，即得

$$(p-1)!\equiv(-1)^r\cdot r!(p-r-1)!.$$

设 r 是一个能使 $(-1)^r\cdot r!\equiv 1 \mod p$ 成立的数，于是有 $(p-1)!\equiv(p-r-1)! \mod p$. 但由威尔逊定理可知

$$(p-1)!+1\equiv 0 \mod p.$$

从而 $(p-r-1)!+1\equiv 0 \mod p$.

容易验证，对 $r=7$ 来说，$(-1)^r\cdot r!\equiv 1 \mod 71$，因而

$$(71-7-1)!+1=63!+1\equiv 0 \mod 71.$$

另外，由于 $8\cdot 9\equiv 1 \mod 71$，$(-1)^9\cdot 9!\equiv 1 \mod 71$，于是

$$(71-9-1)!+1=61!+1\equiv 0 \mod 71.$$

98. 前 n 个连续数的乘积为 $n!$，和为 $[n(n+1)]/2$. 我们应证明 $n!/[n(n+1)/2]=2(n-1)!/(n+1)$ 为一整数.

(a) 若 $(n+1)$ 是合数，阶乘中所可能有的最大素因子是 $(n+1)/2$，它是不可能超过 $(n-1)$ 的（除非 $n=1,2$；但此时 $n+1$ 不是合数）. 因此，$(n-1)!$ 中必含有 $(n+1)/2$，于是 $2(n-1)!/(n+1)$ 为一整数.

(b) 若 $(n+1)$ 含有两个相等因子（最坏的情况是两个奇素数），于是 $(n+1)$ 为一平方数，我们需要证明分子中也含有这两个因子 $(n+1)^{\frac{1}{2}}$. 由于 $n>3$ 时，$(n+1)^{\frac{1}{2}}<(n-1)$，而 $n>7$ 时，$2(n+1)^{\frac{1}{2}}<(n-1)$. 因此 $2(n-1)!$ 中含有两个因子 $(n+1)^{\frac{1}{2}}$ 与 $2(n+1)^{\frac{1}{2}}$，从而还是能被 $(n+1)$ 整除.（$n=1,2,4,5,6$ 时，$(n+1)$ 不是平方数；$n=3$ 时，$2[2!]/4$ 为一整数.）

(c) 最后，当 $(n+1)$ 为素数时，它必大于 $(n-1)!$ 中所含的最大素数，所以这是唯一的一种情况，这时前 n 个连续数的乘积不能为其和数整除.

99. 为了算出 10000! 尾部紧挨着的 0 的个数，只要去算一下 5，25，125，…的倍数个数就行了，因为对于这些数目，我们总能找到一个 2 的幂与之匹配以便得出 10 的乘幂，而 2 的乘幂显然远远多于 5 的乘幂，因此共有 $[10000/5]+[10000/25]+[10000/125]+[10000/625]+[10000/3125]=2000+400+80+16+3=2499$ 个零.

这里，$[a/b]$ 表示不大于 a/b 的最大整数.

100. 等腰直角三角形的每条直角边都具有 m^2+n^2 的形式，因而斜边是 $\sqrt{2}(m^2+n^2)$. 需要证明：存在一个有整数边 x,y

的直角三角形，以使得 $x^2+y^2=2(m^2+n^2)^2$. 当 $x=|m^2-n^2+2mn|$，$y=|m^2-n^2-2mn|$时这是可以做到的，因此时有 $x^2+y^2=2m^4+4m^2n^2+2n^4=2(m^2+n^2)^2$. 当 $m=2$，$n=1$ 时，可得出 $x=7$，$y=1$ 作为两直角边，此时斜边为 $5\sqrt{2}$. 等腰直角三角形的每条直角边满足 $m^2+n^2=5$，而斜边也是 $5\sqrt{2}$. 两者都不能算是整数毕氏三角形，但等腰直角三角形的“腰”都等于 5，而后者却是一个 3-4-5 毕氏三角形的斜边，这就满足了题意.

[338]

索　引

说明：1. 其中数字为原书之页码；

2. 仅在各章末尾参考文献中出现，而在正文中未见之人名一律不用中文注音，以便直接查阅原文书刊.

C

[339]

D

E

F

[341]

G

H

[344]

S

[347]

T